Лабораторная работа № 9
Криптосистема RSA: шифрование и ЭЦП.
по курсу «Защита информации»
Группа А-12-18
Нечаев А. А. (вариант 9)

1. Разработать программный модуль для формирования системных параметров RSA (модуль, открытый ключ, секретный ключ) на основе заданных номеров простых чисел: Q = Prime[10000-N], P = Prime[10000+N], где N – номер по списку в группе.

In[1]:=
```
SeedRandom[9]
```
инициализация генератора псевдослучайных чисел
```
Q = Prime[10000 - 9]
```
простое число
```
P = Prime[10000 + 9]
```
простое число
```
rsaParamsModule[Q_, P_] := Module[{openKey, secretKey, n, phi},
```
программный модуль
```
  n = P * Q;
  phi = (Q - 1) * (P - 1);
  openKey = RandomInteger[{1 + 1, phi}];
```
случайное целое число
```
  While[GCD[openKey, phi] ≠ 1, openKey = RandomInteger[{1 + 1, phi}]];
```
цикл… НОД случайное целое число
```
  secretKey = PowerMod[openKey, -1, phi];
```
степень по модулю
```
  While[GCD[secretKey, n] ≠ 1,
```
цикл… НОД
```
   While[GCD[openKey, phi] ≠ 1, openKey = RandomInteger[{1 + 1, phi}]];
```
цикл… НОД случайное целое число
```
   secretKey = PowerMod[openKey, -1, phi]];
```
степень по модулю
```
  Print["N = ", P * Q];
```
печат… численное приближение
```
  Print["Open key = ", openKey];
```
печатать
```
  Print["Secret key = ", secretKey];
```
печатать
```
 ]
rsaParamsModule[Q, P]
```

Out[2]= 104 677

Out[3]= 104 827

N = 10 972 975 879

Open key = 2 396 097 779

Secret key = 4 047 511 979

In[6]:=
```
n = 10 972 975 879
openKey = 2 396 097 779
secretKey = 4 047 511 979
```

Out[6]= 10 972 975 879

Out[7]= 2 396 097 779

Out[8]= 4 047 511 979

2. Импортировать текстовый файл Text-N с номером по списку в группе из папки Plaintext1RSA. Провести анализ кодов текста и привести к виду : 1XXX или 2XXX - четыре десятичных цифры, представляющие собой блок для шифрования в RSA. Например: код пробела 32 представляем как 2000+32=2032.

In[9]:=
```
msgText = "из возможности
    возникновения наиболее опасной ситуации, обусловленной действиями нарушителя,
    можно составить гипотетическую модель потенциального нарушителя  [57]:
• квалификация нарушителя может быть на уровне разработчика данной системы;
• нарушителем может быть как постороннее лицо, так и законный пользователь системы;
• нарушителю известна информация о принципах работы системы;
• нарушитель выберет наиболее слабое звено в защите.
\tВ частности, для банковских АСОИ можно выделить следующие преднамеренные угрозы:
• несанкционированный доступ посторонних лиц,
    не принадлежащих к числу банковских служащих,
    и ознакомление с хранимой конфиденциальной информацией;
• ознакомление банковских служащих с информацией,
    к которой они не должны иметь доступ;
• несанкционированное копирование программ и данных;
• кража магнитных носителей, содержащих конфиденциальную информацию;
• кража распечатанных банковских документов;
• умышленное уничтожение информации;
• несанкционированная модификация банковскими служащими финансовых документов,
    отчетности и баз данных;
• фальсификация сообщений, передаваемых по каналам связи;
• отказ от авторства сообщения, переданного по каналам связи;
• отказ от факта получения информации;
• навязывание ранее переданного сообщения;
•";
msgCodeList = ToCharacterCode[msgText];
                  код символа
Do[If[msgCodeList[[i]] < 1000, msgCodeList[[i]] += 2000], {i, 1, Length[msgCodeList]}]
  ···  условный оператор                                                  длина
Tally[msgCodeList][[All, 1]]
подсчитать                 всё
```

Out[12]=
```
{1080, 1079, 2032, 1074, 1086, 1084, 1078, 1085, 1089, 1090, 1082,
 1077, 1103, 1072, 1073, 1083, 1087, 1081, 1091, 1094, 2044, 1076, 1088,
 1096, 1100, 1075, 1095, 1102, 2091, 2053, 2055, 2093, 2058, 2010, 8226,
 1092, 1099, 2059, 1093, 1097, 2046, 2009, 1042, 1040, 1057, 1054, 1048}
```

In[14]:=
```
N[Entropy[2, msgCodeList]]
 ··  энтропия
```

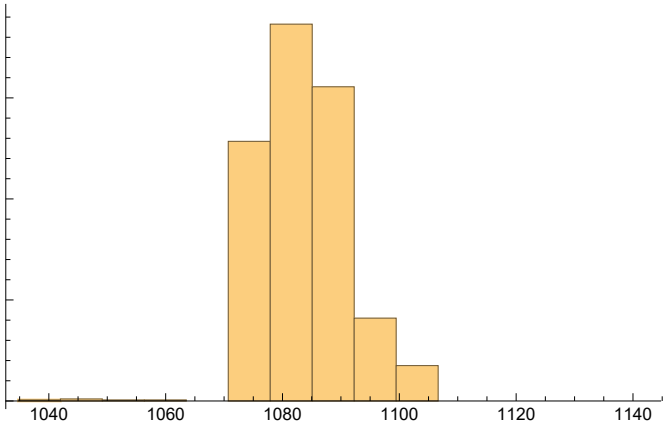
Out[14]= 4.64524

(энтропия текста)

3. Построить гистограмму распределения кодов символов открытого текста.

In[15]:=
```
Histogram[msgCodeList]
```
гистограмма

Out[15]=



4. Зашифровать текст на открытом ключе и определить энтропию шифртекста.

In[16]:=
```
cryptCodeList = {};
Do[
```
оператор цикла
```
 AppendTo[
```
добавить в конец к
```
  cryptCodeList,
  PowerMod[msgCodeList[[i]], openKey, n]], {i, 1, Length[msgCodeList]}]
```
степень по модулю, длина
```
cryptCodeList
```

Out[18]=
```
{8 269 408 948, 10 335 062 019, 1 371 786 632, 5 031 693 195, 8 423 997 243, 10 335 062 019,
 10 080 607 259, 8 423 997 243, 2 956 058 005, 1 384 365 383, 8 423 997 243, 1 833 384 701,
 3 080 625 892, 8 269 408 948, 1 371 786 632, 5 031 693 195, 8 423 997 243, 10 335 062 019,
 1 384 365 383, 8 269 408 948, 7 072 646 935, 1 384 365 383, 8 423 997 243, 5 031 693 195,
 1 510 212 228, 1 384 365 383, 8 269 408 948, 5 843 238 561, 1 371 786 632, 1 384 365 383,
 8 564 868 140, 8 269 408 948, 3 735 108 414, 8 423 997 243, 2 944 906 221, 1 510 212 228,
 1 510 212 228, 1 371 786 632, 8 423 997 243, 9 256 725 952, 8 564 868 140, 1 833 384 701,
 1 384 365 383, 8 423 997 243, 2 752 289 270, 1 371 786 632, 1 833 384 701, 8 269 408 948,
 3 080 625 892, 2 132 919 721, 8 564 868 140, 4 180 200 535, 8 269 408 948, 8 269 408 948,
 778 707 549, 1 371 786 632, 8 423 997 243, 3 735 108 414, 2 132 919 721, 1 833 384 701,
 2 944 906 221, 8 423 997 243, 5 031 693 195, 2 944 906 221, 1 510 212 228, 1 384 365 383,
 1 384 365 383, 8 423 997 243, 2 752 289 270, 1 371 786 632, 4 780 460 291, 1 510 212 228,
 2 752 289 270, 1 833 384 701, 3 080 625 892, 5 031 693 195, 8 269 408 948, 5 843 238 561,
 10 080 607 259, 8 269 408 948, 1 371 786 632, 1 384 365 383, 8 564 868 140, 1 838 373 661,
 2 132 919 721, 1 896 860 349, 8 269 408 948, 3 080 625 892, 1 510 212 228, 2 944 906 221,
 5 843 238 561, 778 707 549, 1 371 786 632, 10 080 607 259, 8 423 997 243, 2 956 058 005,
 1 384 365 383, 8 423 997 243, 1 371 786 632, 1 833 384 701, 8 423 997 243, 1 833 384 701,
 3 080 625 892, 8 564 868 140, 5 031 693 195, 8 269 408 948, 3 080 625 892, 2 959 925 561,
 1 371 786 632, 8 418 819 156, 8 269 408 948, 9 256 725 952, 8 423 997 243, 3 080 625 892,
 1 510 212 228, 3 080 625 892, 8 269 408 948, 1 547 726 557, 1 510 212 228, 1 833 384 701,
 7 072 646 935, 2 132 919 721, 7 394 622 051, 1 371 786 632, 10 080 607 259, 8 423 997 243,
 4 780 460 291, 1 510 212 228, 2 944 906 221, 2 959 925 561, 1 371 786 632, 9 256 725 952,
 8 423 997 243, 3 080 625 892, 1 510 212 228, 1 384 365 383, 4 180 200 535, 8 269 408 948,
 8 564 868 140, 2 944 906 221, 2 959 925 561, 1 384 365 383, 8 423 997 243, 8 418 819 156,
 8 423 997 243, 1 371 786 632, 1 384 365 383, 8 564 868 140, 1 838 373 661, 2 132 919 721,
 1 896 860 349, 8 269 408 948, 3 080 625 892, 1 510 212 228, 2 944 906 221, 5 843 238 561,
 1 371 786 632, 1 371 786 632, 7 720 400 704, 6 632 567 772, 5 372 278 671, 10 772 100 615,
```

5 237 864 101, 6 491 726 779, 5 456 877 370, 1 371 786 632, 7 072 646 935, 5 031 693 195,
8 564 868 140, 2 944 906 221, 8 269 408 948, 2 603 733 967, 8 269 408 948, 7 072 646 935,
8 564 868 140, 4 180 200 535, 8 269 408 948, 5 843 238 561, 1 371 786 632, 1 384 365 383,
8 564 868 140, 1 838 373 661, 2 132 919 721, 1 896 860 349, 8 269 408 948, 3 080 625 892,
1 510 212 228, 2 944 906 221, 5 843 238 561, 1 371 786 632, 10 080 607 259, 8 423 997 243,
2 956 058 005, 1 510 212 228, 3 080 625 892, 1 371 786 632, 3 735 108 414, 7 817 091 098,
3 080 625 892, 2 959 925 561, 1 371 786 632, 1 384 365 383, 8 564 868 140, 1 371 786 632,
2 132 919 721, 1 838 373 661, 8 423 997 243, 5 031 693 195, 1 384 365 383, 1 510 212 228,
1 371 786 632, 1 838 373 661, 8 564 868 140, 10 335 062 019, 1 838 373 661, 8 564 868 140,
3 735 108 414, 8 423 997 243, 3 080 625 892, 1 547 726 557, 8 269 408 948, 7 072 646 935,
8 564 868 140, 1 371 786 632, 4 780 460 291, 8 564 868 140, 1 384 365 383, 1 384 365 383,
8 423 997 243, 2 752 289 270, 1 371 786 632, 1 833 384 701, 8 269 408 948, 1 833 384 701,
3 080 625 892, 1 510 212 228, 10 080 607 259, 7 817 091 098, 6 348 106 759, 6 491 726 779,
5 456 877 370, 1 371 786 632, 1 384 365 383, 8 564 868 140, 1 838 373 661, 2 132 919 721,
1 896 860 349, 8 269 408 948, 3 080 625 892, 1 510 212 228, 2 944 906 221, 1 510 212 228,
10 080 607 259, 1 371 786 632, 10 080 607 259, 8 423 997 243, 2 956 058 005, 1 510 212 228,
3 080 625 892, 1 371 786 632, 3 735 108 414, 7 817 091 098, 3 080 625 892, 2 959 925 561,
1 371 786 632, 7 072 646 935, 8 564 868 140, 7 072 646 935, 1 371 786 632, 9 256 725 952,
8 423 997 243, 1 833 384 701, 3 080 625 892, 8 423 997 243, 1 838 373 661, 8 423 997 243,
1 384 365 383, 1 384 365 383, 1 510 212 228, 1 510 212 228, 1 371 786 632, 2 944 906 221,
8 269 408 948, 4 180 200 535, 8 423 997 243, 778 707 549, 1 371 786 632, 3 080 625 892,
8 564 868 140, 7 072 646 935, 1 371 786 632, 8 269 408 948, 1 371 786 632, 10 335 062 019,
8 564 868 140, 7 072 646 935, 8 423 997 243, 1 384 365 383, 1 384 365 383, 7 817 091 098,
2 752 289 270, 1 371 786 632, 9 256 725 952, 8 423 997 243, 2 944 906 221, 2 959 925 561,
10 335 062 019, 8 423 997 243, 5 031 693 195, 8 564 868 140, 3 080 625 892, 1 510 212 228,
2 944 906 221, 2 959 925 561, 1 371 786 632, 1 833 384 701, 8 269 408 948, 1 833 384 701,
3 080 625 892, 1 510 212 228, 10 080 607 259, 7 817 091 098, 6 348 106 759, 6 491 726 779,
5 456 877 370, 1 371 786 632, 1 384 365 383, 8 564 868 140, 1 838 373 661, 2 132 919 721,
1 896 860 349, 8 269 408 948, 3 080 625 892, 1 510 212 228, 2 944 906 221, 7 394 622 051,
1 371 786 632, 8 269 408 948, 10 335 062 019, 5 031 693 195, 1 510 212 228, 1 833 384 701,
3 080 625 892, 1 384 365 383, 8 564 868 140, 1 371 786 632, 8 269 408 948, 1 384 365 383,
2 603 733 967, 8 423 997 243, 1 838 373 661, 10 080 607 259, 8 564 868 140, 4 180 200 535,
8 269 408 948, 5 843 238 561, 1 371 786 632, 8 423 997 243, 1 371 786 632, 9 256 725 952,
1 838 373 661, 8 269 408 948, 1 384 365 383, 4 180 200 535, 8 269 408 948, 9 256 725 952,
8 564 868 140, 9 397 849 264, 1 371 786 632, 1 838 373 661, 8 564 868 140, 3 735 108 414,
8 423 997 243, 3 080 625 892, 7 817 091 098, 1 371 786 632, 1 833 384 701, 8 269 408 948,
1 833 384 701, 3 080 625 892, 1 510 212 228, 10 080 607 259, 7 817 091 098, 6 348 106 759,
6 491 726 779, 5 456 877 370, 1 371 786 632, 1 384 365 383, 8 564 868 140, 1 838 373 661,
2 132 919 721, 1 896 860 349, 8 269 408 948, 3 080 625 892, 1 510 212 228, 2 944 906 221,
2 959 925 561, 1 371 786 632, 5 031 693 195, 7 817 091 098, 3 735 108 414, 1 510 212 228,
1 838 373 661, 1 510 212 228, 3 080 625 892, 1 371 786 632, 1 384 365 383, 8 564 868 140,
8 269 408 948, 3 735 108 414, 8 423 997 243, 2 944 906 221, 1 510 212 228, 1 510 212 228,
1 371 786 632, 1 833 384 701, 2 944 906 221, 8 564 868 140, 3 735 108 414, 8 423 997 243,
1 510 212 228, 1 371 786 632, 10 335 062 019, 5 031 693 195, 1 510 212 228, 1 384 365 383,
8 423 997 243, 1 371 786 632, 5 031 693 195, 1 371 786 632, 10 335 062 019, 8 564 868 140,
39 649 894, 8 269 408 948, 3 080 625 892, 1 510 212 228, 1 091 508 623, 6 491 726 779,
4 911 925 501, 8 331 733 052, 1 371 786 632, 1 547 726 557, 8 564 868 140, 1 833 384 701,
3 080 625 892, 1 384 365 383, 8 423 997 243, 1 833 384 701, 3 080 625 892, 8 269 408 948,
778 707 549, 1 371 786 632, 4 780 460 291, 2 944 906 221, 5 843 238 561, 1 371 786 632,
3 735 108 414, 8 564 868 140, 1 384 365 383, 7 072 646 935, 8 423 997 243, 5 031 693 195,
1 833 384 701, 7 072 646 935, 8 269 408 948, 9 397 849 264, 1 371 786 632, 6 083 484 343,
3 611 380 048, 4 735 460 115, 8 670 758 099, 1 371 786 632, 10 080 607 259, 8 423 997 243,
2 956 058 005, 1 384 365 383, 8 423 997 243, 1 371 786 632, 5 031 693 195, 7 817 091 098,
4 780 460 291, 1 510 212 228, 2 944 906 221, 8 269 408 948, 3 080 625 892, 2 959 925 561,
1 371 786 632, 1 833 384 701, 2 944 906 221, 1 510 212 228, 4 780 460 291, 2 132 919 721,

7 394 622 051, 39 649 894, 8 269 408 948, 1 510 212 228, 1 371 786 632, 9 256 725 952,
1 838 373 661, 1 510 212 228, 4 780 460 291, 1 384 365 383, 8 564 868 140, 10 080 607 259,
1 510 212 228, 1 838 373 661, 1 510 212 228, 1 384 365 383, 1 384 365 383, 7 817 091 098,
1 510 212 228, 1 371 786 632, 2 132 919 721, 8 418 819 156, 1 838 373 661, 8 423 997 243,
10 335 062 019, 7 817 091 098, 5 237 864 101, 6 491 726 779, 5 456 877 370, 1 371 786 632,
1 384 365 383, 1 510 212 228, 1 833 384 701, 8 564 868 140, 1 384 365 383, 7 072 646 935,
4 180 200 535, 8 269 408 948, 8 423 997 243, 1 384 365 383, 8 269 408 948, 1 838 373 661,
8 423 997 243, 5 031 693 195, 8 564 868 140, 1 384 365 383, 1 384 365 383, 7 817 091 098,
2 752 289 270, 1 371 786 632, 4 780 460 291, 8 423 997 243, 1 833 384 701, 3 080 625 892,
2 132 919 721, 9 256 725 952, 1 371 786 632, 9 256 725 952, 8 423 997 243, 1 833 384 701,
3 080 625 892, 8 423 997 243, 1 838 373 661, 8 423 997 243, 1 384 365 383, 1 384 365 383,
8 269 408 948, 9 397 849 264, 1 371 786 632, 2 944 906 221, 8 269 408 948, 4 180 200 535,
778 707 549, 1 371 786 632, 1 384 365 383, 1 510 212 228, 1 371 786 632, 9 256 725 952,
1 838 373 661, 8 269 408 948, 1 384 365 383, 8 564 868 140, 4 780 460 291, 2 944 906 221,
1 510 212 228, 2 956 058 005, 8 564 868 140, 39 649 894, 8 269 408 948, 9 397 849 264,
1 371 786 632, 7 072 646 935, 1 371 786 632, 1 547 726 557, 8 269 408 948, 1 833 384 701,
2 944 906 221, 2 132 919 721, 1 371 786 632, 3 735 108 414, 8 564 868 140, 1 384 365 383,
7 072 646 935, 8 423 997 243, 5 031 693 195, 1 833 384 701, 7 072 646 935, 8 269 408 948,
9 397 849 264, 1 371 786 632, 1 833 384 701, 2 944 906 221, 2 132 919 721, 2 956 058 005,
8 564 868 140, 39 649 894, 8 269 408 948, 9 397 849 264, 778 707 549, 1 371 786 632, 8 269 408 948,
1 371 786 632, 8 423 997 243, 10 335 062 019, 1 384 365 383, 8 564 868 140, 7 072 646 935,
8 423 997 243, 10 080 607 259, 2 944 906 221, 1 510 212 228, 1 384 365 383, 8 269 408 948,
1 510 212 228, 1 371 786 632, 1 833 384 701, 1 371 786 632, 9 397 849 264, 1 838 373 661,
8 564 868 140, 1 384 365 383, 8 269 408 948, 10 080 607 259, 8 423 997 243, 2 752 289 270,
1 371 786 632, 7 072 646 935, 8 423 997 243, 1 384 365 383, 2 603 733 967, 8 269 408 948,
4 780 460 291, 1 510 212 228, 1 384 365 383, 4 180 200 535, 8 269 408 948, 8 564 868 140,
2 944 906 221, 2 959 925 561, 1 384 365 383, 8 423 997 243, 2 752 289 270, 1 371 786 632,
8 269 408 948, 1 384 365 383, 2 603 733 967, 8 423 997 243, 1 838 373 661, 10 080 607 259,
8 564 868 140, 4 180 200 535, 8 269 408 948, 1 510 212 228, 2 752 289 270, 6 348 106 759,
6 491 726 779, 5 456 877 370, 1 371 786 632, 8 423 997 243, 10 335 062 019, 1 384 365 383,
8 564 868 140, 7 072 646 935, 8 423 997 243, 10 080 607 259, 2 944 906 221, 1 510 212 228,
1 384 365 383, 8 269 408 948, 1 510 212 228, 1 371 786 632, 3 735 108 414, 8 564 868 140,
1 384 365 383, 7 072 646 935, 8 423 997 243, 5 031 693 195, 1 833 384 701, 7 072 646 935,
8 269 408 948, 9 397 849 264, 1 371 786 632, 1 833 384 701, 2 944 906 221, 2 132 919 721,
2 956 058 005, 8 564 868 140, 39 649 894, 8 269 408 948, 9 397 849 264, 1 371 786 632,
1 833 384 701, 1 371 786 632, 8 269 408 948, 1 384 365 383, 2 603 733 967, 8 423 997 243,
1 838 373 661, 10 080 607 259, 8 564 868 140, 4 180 200 535, 8 269 408 948, 1 510 212 228,
2 752 289 270, 778 707 549, 1 371 786 632, 7 072 646 935, 1 371 786 632, 7 072 646 935,
8 423 997 243, 3 080 625 892, 8 423 997 243, 1 838 373 661, 8 423 997 243, 2 752 289 270,
1 371 786 632, 8 423 997 243, 1 384 365 383, 8 269 408 948, 1 371 786 632, 1 384 365 383,
1 510 212 228, 1 371 786 632, 4 780 460 291, 8 423 997 243, 2 944 906 221, 2 956 058 005,
1 384 365 383, 7 817 091 098, 1 371 786 632, 8 269 408 948, 10 080 607 259, 1 510 212 228,
3 080 625 892, 2 959 925 561, 1 371 786 632, 4 780 460 291, 8 423 997 243, 1 833 384 701,
3 080 625 892, 2 132 919 721, 9 256 725 952, 6 348 106 759, 6 491 726 779, 5 456 877 370,
1 371 786 632, 1 384 365 383, 1 510 212 228, 1 833 384 701, 8 564 868 140, 1 384 365 383,
7 072 646 935, 4 180 200 535, 8 269 408 948, 8 423 997 243, 1 384 365 383, 8 269 408 948,
1 838 373 661, 8 423 997 243, 5 031 693 195, 8 564 868 140, 1 384 365 383, 1 384 365 383,
8 423 997 243, 1 510 212 228, 1 371 786 632, 7 072 646 935, 8 423 997 243, 9 256 725 952,
8 269 408 948, 1 838 373 661, 8 423 997 243, 5 031 693 195, 8 564 868 140, 1 384 365 383,
8 269 408 948, 1 510 212 228, 1 371 786 632, 9 256 725 952, 1 838 373 661, 8 423 997 243,
8 418 819 156, 1 838 373 661, 8 564 868 140, 10 080 607 259, 10 080 607 259, 1 371 786 632,
8 269 408 948, 1 371 786 632, 4 780 460 291, 8 564 868 140, 1 384 365 383, 1 384 365 383,
7 817 091 098, 9 397 849 264, 6 348 106 759, 6 491 726 779, 5 456 877 370, 1 371 786 632,
7 072 646 935, 1 838 373 661, 8 564 868 140, 2 956 058 005, 8 564 868 140, 1 371 786 632,
10 080 607 259, 8 564 868 140, 8 418 819 156, 1 384 365 383, 8 269 408 948, 3 080 625 892,

1 384 365 383, 7 817 091 098, 9 397 849 264, 1 371 786 632, 1 384 365 383, 8 423 997 243,
1 833 384 701, 8 269 408 948, 3 080 625 892, 1 510 212 228, 2 944 906 221, 1 510 212 228,
2 752 289 270, 778 707 549, 1 371 786 632, 1 833 384 701, 8 423 997 243, 4 780 460 291,
1 510 212 228, 1 838 373 661, 2 956 058 005, 8 564 868 140, 39 649 894, 8 269 408 948,
9 397 849 264, 1 371 786 632, 7 072 646 935, 8 423 997 243, 1 384 365 383, 2 603 733 967,
8 269 408 948, 4 780 460 291, 1 510 212 228, 1 384 365 383, 4 180 200 535, 8 269 408 948,
8 564 868 140, 2 944 906 221, 2 959 925 561, 1 384 365 383, 2 132 919 721, 7 394 622 051,
1 371 786 632, 8 269 408 948, 1 384 365 383, 2 603 733 967, 8 423 997 243, 1 838 373 661,
10 080 607 259, 8 564 868 140, 4 180 200 535, 8 269 408 948, 7 394 622 051, 6 348 106 759,
6 491 726 779, 5 456 877 370, 1 371 786 632, 7 072 646 935, 1 838 373 661, 8 564 868 140,
2 956 058 005, 8 564 868 140, 1 371 786 632, 1 838 373 661, 8 564 868 140, 1 833 384 701,
9 256 725 952, 1 510 212 228, 1 547 726 557, 8 564 868 140, 3 080 625 892, 8 564 868 140,
1 384 365 383, 1 384 365 383, 7 817 091 098, 9 397 849 264, 1 371 786 632, 3 735 108 414,
8 564 868 140, 1 384 365 383, 7 072 646 935, 8 423 997 243, 5 031 693 195, 1 833 384 701,
7 072 646 935, 8 269 408 948, 9 397 849 264, 1 371 786 632, 4 780 460 291, 8 423 997 243,
7 072 646 935, 2 132 919 721, 10 080 607 259, 1 510 212 228, 1 384 365 383, 3 080 625 892,
8 423 997 243, 5 031 693 195, 6 348 106 759, 6 491 726 779, 5 456 877 370, 1 371 786 632,
2 132 919 721, 10 080 607 259, 7 817 091 098, 1 896 860 349, 2 944 906 221, 1 510 212 228,
1 384 365 383, 1 384 365 383, 8 423 997 243, 1 510 212 228, 1 371 786 632, 2 132 919 721,
1 384 365 383, 8 269 408 948, 1 547 726 557, 3 080 625 892, 8 423 997 243, 2 956 058 005,
1 510 212 228, 1 384 365 383, 8 269 408 948, 1 510 212 228, 1 371 786 632, 8 269 408 948,
1 384 365 383, 2 603 733 967, 8 423 997 243, 1 838 373 661, 10 080 607 259, 8 564 868 140,
4 180 200 535, 8 269 408 948, 8 269 408 948, 6 348 106 759, 6 491 726 779, 5 456 877 370,
1 371 786 632, 1 384 365 383, 1 510 212 228, 1 833 384 701, 8 564 868 140, 1 384 365 383,
7 072 646 935, 4 180 200 535, 8 269 408 948, 8 423 997 243, 1 384 365 383, 8 269 408 948,
1 838 373 661, 8 423 997 243, 5 031 693 195, 8 564 868 140, 1 384 365 383, 1 384 365 383,
8 564 868 140, 5 843 238 561, 1 371 786 632, 10 080 607 259, 8 423 997 243, 4 780 460 291,
8 269 408 948, 2 603 733 967, 8 269 408 948, 7 072 646 935, 8 564 868 140, 4 180 200 535,
8 269 408 948, 5 843 238 561, 1 371 786 632, 3 735 108 414, 8 564 868 140, 1 384 365 383,
7 072 646 935, 8 423 997 243, 5 031 693 195, 1 833 384 701, 7 072 646 935, 8 269 408 948,
10 080 607 259, 8 269 408 948, 1 371 786 632, 1 833 384 701, 2 944 906 221, 2 132 919 721,
2 956 058 005, 8 564 868 140, 39 649 894, 8 269 408 948, 10 080 607 259, 8 269 408 948,
1 371 786 632, 2 603 733 967, 8 269 408 948, 1 384 365 383, 8 564 868 140, 1 384 365 383,
1 833 384 701, 8 423 997 243, 5 031 693 195, 7 817 091 098, 9 397 849 264, 1 371 786 632,
4 780 460 291, 8 423 997 243, 7 072 646 935, 2 132 919 721, 10 080 607 259, 1 510 212 228,
1 384 365 383, 3 080 625 892, 8 423 997 243, 5 031 693 195, 778 707 549, 1 371 786 632,
8 423 997 243, 3 080 625 892, 1 547 726 557, 1 510 212 228, 3 080 625 892, 1 384 365 383,
8 423 997 243, 1 833 384 701, 3 080 625 892, 8 269 408 948, 1 371 786 632, 8 269 408 948,
1 371 786 632, 3 735 108 414, 8 564 868 140, 10 335 062 019, 1 371 786 632, 4 780 460 291,
8 564 868 140, 1 384 365 383, 1 384 365 383, 7 817 091 098, 9 397 849 264, 6 348 106 759,
6 491 726 779, 5 456 877 370, 1 371 786 632, 2 603 733 967, 8 564 868 140, 2 944 906 221,
2 959 925 561, 1 833 384 701, 8 269 408 948, 2 603 733 967, 8 269 408 948, 7 072 646 935,
8 564 868 140, 4 180 200 535, 8 269 408 948, 5 843 238 561, 1 371 786 632, 1 833 384 701,
8 423 997 243, 8 423 997 243, 3 735 108 414, 39 649 894, 1 510 212 228, 1 384 365 383,
8 269 408 948, 2 752 289 270, 778 707 549, 1 371 786 632, 9 256 725 952, 1 510 212 228,
1 838 373 661, 1 510 212 228, 4 780 460 291, 8 564 868 140, 5 031 693 195, 8 564 868 140,
1 510 212 228, 10 080 607 259, 7 817 091 098, 9 397 849 264, 1 371 786 632, 9 256 725 952,
8 423 997 243, 1 371 786 632, 7 072 646 935, 8 564 868 140, 1 384 365 383, 8 564 868 140,
2 944 906 221, 8 564 868 140, 10 080 607 259, 1 371 786 632, 1 833 384 701, 5 031 693 195,
5 843 238 561, 10 335 062 019, 8 269 408 948, 6 348 106 759, 6 491 726 779, 5 456 877 370,
1 371 786 632, 8 423 997 243, 3 080 625 892, 7 072 646 935, 8 564 868 140, 10 335 062 019,
1 371 786 632, 8 423 997 243, 3 080 625 892, 1 371 786 632, 8 564 868 140, 5 031 693 195,
3 080 625 892, 8 423 997 243, 1 838 373 661, 1 833 384 701, 3 080 625 892, 5 031 693 195,
8 564 868 140, 1 371 786 632, 1 833 384 701, 8 423 997 243, 8 423 997 243, 3 735 108 414,
39 649 894, 1 510 212 228, 1 384 365 383, 8 269 408 948, 5 843 238 561, 778 707 549,

```
1 371 786 632, 9 256 725 952, 1 510 212 228, 1 838 373 661, 1 510 212 228, 4 780 460 291,
8 564 868 140, 1 384 365 383, 1 384 365 383, 8 423 997 243, 8 418 819 156, 8 423 997 243,
1 371 786 632, 9 256 725 952, 8 423 997 243, 1 371 786 632, 7 072 646 935, 8 564 868 140,
1 384 365 383, 8 564 868 140, 2 944 906 221, 8 564 868 140, 10 080 607 259, 1 371 786 632,
1 833 384 701, 5 031 693 195, 5 843 238 561, 10 335 062 019, 8 269 408 948, 6 348 106 759,
6 491 726 779, 5 456 877 370, 1 371 786 632, 8 423 997 243, 3 080 625 892, 7 072 646 935,
8 564 868 140, 10 335 062 019, 1 371 786 632, 8 423 997 243, 3 080 625 892, 1 371 786 632,
2 603 733 967, 8 564 868 140, 7 072 646 935, 3 080 625 892, 8 564 868 140, 1 371 786 632,
9 256 725 952, 8 423 997 243, 2 944 906 221, 2 132 919 721, 1 547 726 557, 1 510 212 228,
1 384 365 383, 8 269 408 948, 5 843 238 561, 1 371 786 632, 8 269 408 948, 1 384 365 383,
2 603 733 967, 8 423 997 243, 1 838 373 661, 10 080 607 259, 8 564 868 140, 4 180 200 535,
8 269 408 948, 8 269 408 948, 6 348 106 759, 6 491 726 779, 5 456 877 370, 1 371 786 632,
1 384 365 383, 8 564 868 140, 5 031 693 195, 5 843 238 561, 10 335 062 019, 7 817 091 098,
5 031 693 195, 8 564 868 140, 1 384 365 383, 8 269 408 948, 1 510 212 228, 1 371 786 632,
1 838 373 661, 8 564 868 140, 1 384 365 383, 1 510 212 228, 1 510 212 228, 1 371 786 632,
9 256 725 952, 1 510 212 228, 1 838 373 661, 1 510 212 228, 4 780 460 291, 8 564 868 140,
1 384 365 383, 1 384 365 383, 8 423 997 243, 8 418 819 156, 8 423 997 243, 1 371 786 632,
1 833 384 701, 8 423 997 243, 8 423 997 243, 3 735 108 414, 39 649 894, 1 510 212 228,
1 384 365 383, 8 269 408 948, 5 843 238 561, 6 348 106 759, 6 491 726 779, 5 456 877 370}
```

In[19]:=
```
N[Entropy[2, cryptCodeList]]
```
энтропия

Out[19]=
```
4.64524
```

(энтропии открытого текста и шифртекста равны 4.64524)

5. Провести расшифрование на секретном ключе.

In[20]:=
```
msgCodeList = Table[0, {i, Length[cryptCodeList]}];
              таблица знач… длина
Do[msgCodeList[[i]] = PowerMod[cryptCodeList[[i]], secretKey, n],
оператор цикла              степень по модулю
  {i, 1, Length[cryptCodeList]}];
         длина
Do[If[msgCodeList[[i]] ≥ 2000 && msgCodeList[[i]] < 3000, msgCodeList[[i]] -= 2000],
… условный оператор
  {i, 1, Length[msgCodeList]}];
         длина
FromCharacterCode[msgCodeList]
символ по его коду
```

Out[23]=

из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить гипотетическую модель потенциального нарушителя [57]:

- квалификация нарушителя может быть на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выберет наиболее слабое звено в защите.

В частности, для банковских АСОИ можно выделить следующие преднамеренные угрозы:

- несанкционированный доступ посторонних лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
- ознакомление банковских служащих с информацией, к которой они не должны иметь доступ;
- несанкционированное копирование программ и данных;
- кража магнитных носителей, содержащих конфиденциальную информацию;
- кража распечатанных банковских документов;
- умышленное уничтожение информации;
- несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;
- фальсификация сообщений, передаваемых по каналам связи;
- отказ от авторства сообщения, переданного по каналам связи;
- отказ от факта получения информации;
- навязывание ранее переданного сообщения;
-

(полученный при расшифровке текст совпал с исходным)

6. Сформировать из модифицированных блоков открытого текста (см. п.2) десятичные эквиваленты биграмм: {1079,2032}->{10792032}.

In[24]:=
```
msgText = "из возможности
    возникновения наиболее опасной ситуации, обусловленной действиями нарушителя,
    можно составить гипотетическую модель потенциального нарушителя  [57]:
• квалификация нарушителя может быть на уровне разработчика данной системы;
• нарушителем может быть как постороннее лицо, так и законный пользователь системы;
• нарушителю известна информация о принципах работы системы;
• нарушитель выберет наиболее слабое звено в защите.
\tВ частности, для банковских АСОИ можно выделить следующие преднамеренные угрозы:
• несанкционированный доступ посторонних лиц,
    не принадлежащих к числу банковских служащих,
    и ознакомление с хранимой конфиденциальной информацией;
• ознакомление банковских служащих с информацией,
    к которой они не должны иметь доступ;
• несанкционированное копирование программ и данных;
• кража магнитных носителей, содержащих конфиденциальную информацию;
• кража распечатанных банковских документов;
• умышленное уничтожение информации;
• несанкционированная модификация банковскими служащими финансовых документов,
    отчетности и баз данных;
• фальсификация сообщений, передаваемых по каналам связи;
• отказ от авторства сообщения, переданного по каналам связи;
• отказ от факта получения информации;
• навязывание ранее переданного сообщения;
•";
msgCodeList = ToCharacterCode[msgText];
                код символа
Do[If[msgCodeList[[i]] < 1000, msgCodeList[[i]] += 2000], {i, 1, Length[msgCodeList]}]
… условный оператор                                                  длина
msgCode1List = {};
msgCode2List = {};
Do[
оператор цикла
 AppendTo[msgCode1List, msgCodeList[[2 * i - 1]]];
 добавить в конец к
 AppendTo[msgCode2List, msgCodeList[[2 * i]]],
 добавить в конец к
 {i, 1, IntegerPart[Length[msgCodeList] / 2]}]
        целая часть  длина
msgCodeBinList = msgCode1List * 10 000 + msgCode2List
```

Out[30]=
```
{10 801 079, 20 321 074, 10 861 079, 10 841 086, 10 781 085, 10 861 089, 10 901 080, 20 321 074,
 10 861 079, 10 851 080, 10 821 085, 10 861 074, 10 771 085, 10 801 103, 20 321 085, 10 721 080,
 10 731 086, 10 831 077, 10 772 032, 10 861 087, 10 721 089, 10 851 086, 10 812 032, 10 891 080,
 10 901 091, 10 721 094, 10 801 080, 20 442 032, 10 861 073, 10 911 089, 10 831 086, 10 741 083,
 10 771 085, 10 851 086, 10 812 032, 10 761 077, 10 811 089, 10 901 074, 10 801 103, 10 841 080,
 20 321 085, 10 721 088, 10 911 096, 10 801 090, 10 771 083, 11 032 044, 20 321 084, 10 861 078,
 10 851 086, 20 321 089, 10 861 089, 10 901 072, 10 741 080, 10 901 100, 20 321 075,
 10 801 087, 10 861 090, 10 771 090, 10 801 095, 10 771 089, 10 821 091, 11 022 032,
 10 841 086, 10 761 077, 10 831 100, 20 321 087, 10 861 090, 10 771 085, 10 941 080,
 10 721 083, 11 001 085, 10 861 075, 10 862 032, 10 851 072, 10 881 091, 10 961 080,
 10 901 077, 10 831 103, 20 322 032, 20 912 053, 20 552 093, 20 582 010, 82 262 032,
 10 821 074, 10 721 083, 10 801 092, 10 801 082, 10 721 094, 10 801 103, 20 321 085, 10 721 088,
 10 911 096, 10 801 090, 10 771 083, 11 032 032, 10 841 086, 10 781 077, 10 902 032,
 10 731 099, 10 901 100, 20 321 085, 10 722 032, 10 911 088, 10 861 074, 10 851 077, 20 321 088,
 10 721 079, 10 881 072, 10 731 086, 10 901 095, 10 801 082, 10 722 032, 10 761 072, 10 851 085,
```

10 861 081, 20 321 089, 10 801 089, 10 901 077, 10 841 099, 20 592 010, 82 262 032, 10 851 072,
10 881 091, 10 961 080, 10 901 077, 10 831 077, 10 842 032, 10 841 086, 10 781 077, 10 902 032,
10 731 099, 10 901 100, 20 321 082, 10 721 082, 20 321 087, 10 861 089, 10 901 086, 10 881 086,
10 851 085, 10 771 077, 20 321 083, 10 801 094, 10 862 044, 20 321 090, 10 721 082, 20 321 080,
20 321 079, 10 721 082, 10 861 085, 10 851 099, 10 812 032, 10 871 086, 10 831 100, 10 791 086,
10 741 072, 10 901 077, 10 831 100, 20 321 089, 10 801 089, 10 901 077, 10 841 099, 20 592 010,
82 262 032, 10 851 072, 10 881 091, 10 961 080, 10 901 077, 10 831 102, 20 321 080, 10 791 074,
10 771 089, 10 901 085, 10 722 032, 10 801 085, 10 921 086, 10 881 084, 10 721 094, 10 801 103,
20 321 086, 20 321 087, 10 881 080, 10 851 094, 10 801 087, 10 721 093, 20 321 088, 10 721 073,
10 861 090, 10 992 032, 10 891 080, 10 891 090, 10 771 084, 10 992 059, 20 108 226, 20 321 085,
10 721 088, 10 911 096, 10 801 090, 10 771 083, 11 002 032, 10 741 099, 10 731 077, 10 881 077,
10 902 032, 10 851 072, 10 801 073, 10 861 083, 10 771 077, 20 321 089, 10 831 072, 10 731 086,
10 772 032, 10 791 074, 10 771 085, 10 862 032, 10 742 032, 10 791 072, 10 971 080, 10 901 077,
20 462 010, 20 091 042, 20 321 095, 10 721 089, 10 901 085, 10 861 089, 10 901 080, 20 442 032,
10 761 083, 11 032 032, 10 731 072, 10 851 082, 10 861 074, 10 891 082, 10 801 093, 20 321 040,
10 571 054, 10 482 032, 10 841 086, 10 781 085, 10 862 032, 10 741 099, 10 761 077, 10 831 080,
10 901 100, 20 321 089, 10 831 077, 10 761 091, 11 021 097, 10 801 077, 20 321 087, 10 881 077,
10 761 085, 10 721 084, 10 771 088, 10 771 085, 10 851 099, 10 772 032, 10 911 075, 10 881 086,
10 791 099, 20 582 010, 82 262 032, 10 851 077, 10 891 072, 10 851 082, 10 941 080, 10 861 085,
10 801 088, 10 861 074, 10 721 085, 10 851 099, 10 812 032, 10 761 086, 10 891 090, 10 911 087,
20 321 087, 10 861 089, 10 901 086, 10 881 086, 10 851 085, 10 801 093, 20 321 083, 10 801 094,
20 442 032, 10 851 077, 20 321 087, 10 881 080, 10 851 072, 10 761 083, 10 771 078, 10 721 097,
10 801 093, 20 321 082, 20 321 095, 10 801 089, 10 831 091, 20 321 073, 10 721 085, 10 821 086,
10 741 089, 10 821 080, 10 932 032, 10 891 083, 10 911 078, 10 721 097, 10 801 093, 20 442 032,
10 802 032, 10 861 079, 10 851 072, 10 821 086, 10 841 083, 10 771 085, 10 801 077, 20 321 089,
20 321 093, 10 881 072, 10 851 080, 10 841 086, 10 812 032, 10 821 086, 10 851 092, 10 801 076,
10 771 085, 10 941 080, 10 721 083, 11 001 085, 10 861 081, 20 321 080, 10 851 092, 10 861 088,
10 841 072, 10 941 080, 10 771 081, 20 592 010, 82 262 032, 10 861 079, 10 851 072, 10 821 086,
10 841 083, 10 771 085, 10 801 077, 20 321 073, 10 721 085, 10 821 086, 10 741 089, 10 821 080,
10 932 032, 10 891 083, 10 911 078, 10 721 097, 10 801 093, 20 321 089, 20 321 080, 10 851 092,
10 861 088, 10 841 072, 10 941 080, 10 771 081, 20 442 032, 10 822 032, 10 821 086, 10 901 086,
10 881 086, 10 812 032, 10 861 085, 10 802 032, 10 851 077, 20 321 076, 10 861 083, 10 781 085,
10 992 032, 10 801 084, 10 771 090, 11 002 032, 10 761 086, 10 891 090, 10 911 087, 20 592 010,
82 262 032, 10 851 077, 10 891 072, 10 851 082, 10 941 080, 10 861 085, 10 801 088, 10 861 074,
10 721 085, 10 851 086, 10 772 032, 10 821 086, 10 871 080, 10 881 086, 10 741 072, 10 851 080,
10 772 032, 10 871 088, 10 861 075, 10 881 072, 10 841 084, 20 321 080, 20 321 076, 10 721 085,
10 851 099, 10 932 059, 20 108 226, 20 321 082, 10 881 072, 10 781 072, 20 321 084, 10 721 075,
10 851 080, 10 901 085, 10 991 093, 20 321 085, 10 861 089, 10 801 090, 10 771 083, 10 771 081,
20 442 032, 10 891 086, 10 761 077, 10 881 078, 10 721 097, 10 801 093, 20 321 082, 10 861 085,
10 921 080, 10 761 077, 10 851 094, 10 801 072, 10 831 100, 10 851 091, 11 022 032, 10 801 085,
10 921 086, 10 881 084, 10 721 094, 10 801 102, 20 592 010, 82 262 032, 10 821 088, 10 721 078,
10 722 032, 10 881 072, 10 891 087, 10 771 095, 10 721 090, 10 721 085, 10 851 099, 10 932 032,
10 731 072, 10 851 082, 10 861 074, 10 891 082, 10 801 093, 20 321 076, 10 861 082, 10 911 084,
10 771 085, 10 901 086, 10 742 059, 20 108 226, 20 321 091, 10 841 099, 10 961 083, 10 771 085,
10 851 086, 10 772 032, 10 911 085, 10 801 095, 10 901 086, 10 781 077, 10 851 080, 10 772 032,
10 801 085, 10 921 086, 10 881 084, 10 721 094, 10 801 080, 20 592 010, 82 262 032, 10 851 077,
10 891 072, 10 851 082, 10 941 080, 10 861 085, 10 801 088, 10 861 074, 10 721 085, 10 851 072,
11 032 032, 10 841 086, 10 761 080, 10 921 080, 10 821 072, 10 941 080, 11 032 032, 10 731 072,
10 851 082, 10 861 074, 10 891 082, 10 801 084, 10 802 032, 10 891 083, 10 911 078, 10 721 097,
10 801 084, 10 802 032, 10 921 080, 10 851 072, 10 851 089, 10 861 074, 10 991 093, 20 321 076,
10 861 082, 10 911 084, 10 771 085, 10 901 086, 10 742 044, 20 321 086, 10 901 095, 10 771 090,
10 851 086, 10 891 090, 10 802 032, 10 802 032, 10 731 072, 10 792 032, 10 761 072, 10 851 085,
10 991 093, 20 592 010, 82 262 032, 10 921 072, 10 831 100, 10 891 080, 10 921 080, 10 821 072,
10 941 080, 11 032 032, 10 891 086, 10 861 073, 10 971 077, 10 851 080, 10 812 044, 20 321 087,
10 771 088, 10 771 076, 10 721 074, 10 721 077, 10 841 099, 10 932 032, 10 871 086, 20 321 082,

10 721 085, 10 721 083, 10 721 084, 20 321 089, 10 741 103, 10 791 080, 20 592 010, 82 262 032,
10 861 090, 10 821 072, 10 792 032, 10 861 090, 20 321 072, 10 741 090, 10 861 088, 10 891 090,
10 741 072, 20 321 089, 10 861 086, 10 731 097, 10 771 085, 10 801 103, 20 442 032, 10 871 077,
10 881 077, 10 761 072, 10 851 085, 10 861 075, 10 862 032, 10 871 086, 20 321 082, 10 721 085,
10 721 083, 10 721 084, 20 321 089, 10 741 103, 10 791 080, 20 592 010, 82 262 032, 10 861 090,
10 821 072, 10 792 032, 10 861 090, 20 321 092, 10 721 082, 10 901 072, 20 321 087, 10 861 083,
10 911 095, 10 771 085, 10 801 103, 20 321 080, 10 851 092, 10 861 088, 10 841 072, 10 941 080,
10 802 059, 20 108 226, 20 321 085, 10 721 074, 11 031 079, 10 991 074, 10 721 085, 10 801 077,
20 321 088, 10 721 085, 10 771 077, 20 321 087, 10 771 088, 10 771 076, 10 721 085, 10 851 086,
10 751 086, 20 321 089, 10 861 086, 10 731 097, 10 771 085, 10 801 103, 20 592 010}

7. Провести шифрование блоков биграмм на открытом ключе. Определить энтропию шифр текста.

In[31]:=
```
cryptCodeBinList = {};
Do[AppendTo[cryptCodeBinList, PowerMod[msgCodeBinList[[i]], openKey, n]],
 {i, 1, Length[msgCodeBinList]}]
cryptCodeBinList
```

Out[33]= {5 255 404 247, 2 096 703 867, 5 730 599 267, 2 138 500 761, 10 379 662 225, 1 193 340 762,
4 308 736 040, 2 096 703 867, 5 730 599 267, 5 718 208 827, 5 851 046 379, 3 317 701 700,
3 828 812 904, 9 253 212 916, 8 997 086 152, 8 156 228 230, 2 404 158 496, 5 104 419 925,
325 902 326, 2 384 708 395, 6 420 850 546, 7 657 746 574, 4 734 036 254, 6 770 477 007,
2 783 662 203, 494 238 476, 3 793 008 030, 7 354 163 795, 7 456 014 596, 9 905 110 043,
1 188 301 413, 6 525 968 541, 3 828 812 904, 7 657 746 574, 4 734 036 254, 144 995 288,
2 854 819 204, 858 327 935, 9 253 212 916, 10 714 402 263, 8 997 086 152, 9 076 217 008,
6 304 028 979, 2 240 718 689, 988 101 827, 3 341 109 845, 10 619 632 508, 4 943 459 620,
7 657 746 574, 1 792 417 495, 1 193 340 762, 4 991 458 112, 404 965 654, 6 912 524 814,
819 890 329, 9 684 634 091, 5 443 864 623, 5 119 528 440, 8 406 571 873, 8 603 986 273,
9 536 446 990, 2 245 667 888, 2 138 500 761, 144 995 288, 3 106 462 717, 3 882 688 232,
5 443 864 623, 3 828 812 904, 4 957 339 862, 255 835 867, 7 907 864 609, 10 078 344 535,
5 196 733 899, 7 270 663 960, 4 697 303 462, 6 815 670 064, 10 296 358 905, 3 050 537 408,
3 398 356 035, 7 163 861 345, 4 640 900 211, 4 541 855 639, 1 599 544 013, 5 562 192 582,
255 835 867, 9 119 152 263, 252 773 552, 494 238 476, 9 253 212 916, 8 997 086 152, 9 076 217 008,
6 304 028 979, 2 240 718 689, 988 101 827, 2 360 053 725, 2 138 500 761, 1 532 337 430,
5 644 427 531, 1 731 888 376, 6 912 524 814, 8 997 086 152, 3 702 610 692, 874 141 834,
3 317 701 700, 3 729 366 807, 1 091 052 264, 8 614 630 730, 3 230 641 052, 2 404 158 496,
8 863 444 413, 252 773 552, 3 702 610 692, 4 102 961 260, 7 865 602 013, 2 910 618 717,
1 792 417 495, 10 486 277 362, 10 296 358 905, 75 633 548, 10 067 292 272, 1 599 544 013,
7 270 663 960, 4 697 303 462, 6 815 670 064, 10 296 358 905, 5 104 419 925, 3 838 695 645,
2 138 500 761, 1 532 337 430, 5 644 427 531, 1 731 888 376, 6 912 524 814, 5 410 172 999,
2 948 593 242, 3 882 688 232, 1 193 340 762, 390 113 298, 5 279 260 061, 7 865 602 013,
3 818 626 831, 6 790 350 613, 10 292 526 668, 1 763 826 472, 8 157 123 466, 2 948 593 242,
2 453 237 606, 3 342 367 553, 2 948 593 242, 854 462 070, 1 123 759 675, 4 734 036 254,
6 714 242 794, 3 106 462 717, 9 132 451 466, 9 574 764 296, 10 296 358 905, 3 106 462 717,
1 792 417 495, 10 486 277 362, 10 296 358 905, 75 633 548, 10 067 292 272, 1 599 544 013,
7 270 663 960, 4 697 303 462, 6 815 670 064, 10 296 358 905, 9 652 940 291, 2 453 237 606,
7 847 856 341, 8 603 986 273, 5 705 870 597, 3 702 610 692, 632 745 968, 2 010 848 990,
8 444 897 345, 494 238 476, 9 253 212 916, 4 763 588 374, 3 882 688 232, 5 522 845 986,
3 358 401 938, 9 684 634 091, 3 725 919 158, 1 091 052 264, 1 319 630 358, 5 443 864 623,
10 301 725 279, 6 770 477 007, 6 900 059 215, 9 808 545 930, 4 972 627 833, 8 677 774 150,
8 997 086 152, 9 076 217 008, 6 304 028 979, 2 240 718 689, 988 101 827, 10 179 381 957,
7 232 051 599, 6 423 050 202, 7 457 995 059, 5 644 427 531, 7 270 663 960, 4 734 362 871,
10 241 643 857, 3 818 626 831, 1 792 417 495, 5 514 738 706, 2 404 158 496, 325 902 326,

7 847 856 341, 3 828 812 904, 5 196 733 899, 10 956 556 051, 7 736 421 505, 5 986 062 982,
10 296 358 905, 1 991 654 649, 4 561 145 441, 1 484 571 006, 6 420 850 546, 5 705 870 597,
1 193 340 762, 4 308 736 040, 7 354 163 795, 6 253 486 978, 2 360 053 725, 9 790 984 769,
7 123 681 605, 3 317 701 700, 7 595 812 428, 9 953 075 239, 1 301 473 987, 8 218 185 758,
8 994 897 545, 2 138 500 761, 10 379 662 225, 5 196 733 899, 7 232 051 599, 144 995 288,
6 010 311 206, 6 912 524 814, 1 792 417 495, 5 104 419 925, 4 099 072 526, 6 138 169 537,
1 198 597 571, 3 882 688 232, 7 457 995 059, 1 205 736 282, 3 955 550 344, 728 378 312,
3 828 812 904, 1 123 759 675, 325 902 326, 10 669 261 623, 5 279 260 061, 6 234 511 521,
4 541 855 639, 1 599 544 013, 3 729 366 807, 8 388 070 774, 7 123 681 605, 4 957 339 862,
854 462 070, 3 188 774 179, 3 317 701 700, 5 853 744 121, 1 123 759 675, 4 734 036 254,
3 448 467 349, 6 900 059 215, 6 598 821 190, 3 882 688 232, 1 193 340 762, 390 113 298,
5 279 260 061, 7 865 602 013, 9 953 075 239, 6 790 350 613, 10 292 526 668, 7 354 163 795,
3 729 366 807, 3 882 688 232, 5 522 845 986, 7 270 663 960, 6 253 486 978, 5 209 722 432,
10 334 347 023, 9 953 075 239, 5 410 172 999, 1 484 571 006, 10 486 277 362, 2 750 719 859,
1 749 022 572, 5 853 744 121, 6 801 852 381, 7 906 955 782, 5 245 728 995, 6 243 001 278,
2 973 094 056, 3 740 872 486, 10 334 347 023, 9 953 075 239, 7 354 163 795, 5 980 512 470,
5 730 599 267, 7 270 663 960, 6 801 852 381, 9 698 558 410, 3 828 812 904, 1 198 597 571,
1 792 417 495, 10 960 979 830, 3 230 641 052, 5 718 208 827, 2 138 500 761, 4 734 036 254,
6 801 852 381, 4 940 117 279, 10 722 159 320, 3 828 812 904, 4 957 339 862, 255 835 867,
7 907 864 609, 2 910 618 717, 2 453 237 606, 4 940 117 279, 8 801 974 590, 2 531 174 014,
4 957 339 862, 8 841 825 481, 10 067 292 272, 1 599 544 013, 5 730 599 267, 7 270 663 960,
6 801 852 381, 9 698 558 410, 3 828 812 904, 1 198 597 571, 1 749 022 572, 5 853 744 121,
6 801 852 381, 7 906 955 782, 5 245 728 995, 6 243 001 278, 2 973 094 056, 3 740 872 486,
10 334 347 023, 9 953 075 239, 1 792 417 495, 2 453 237 606, 4 940 117 279, 8 801 974 590,
2 531 174 014, 4 957 339 862, 8 841 825 481, 7 354 163 795, 528 663 042, 6 801 852 381,
390 113 298, 5 279 260 061, 4 734 036 254, 854 462 070, 5 980 512 470, 3 729 366 807,
7 061 103 837, 10 241 643 857, 10 379 662 225, 10 301 725 279, 1 811 196 615, 5 119 528 440,
10 179 381 957, 3 448 467 349, 6 900 059 215, 6 598 821 190, 10 067 292 272, 1 599 544 013,
3 729 366 807, 8 388 070 774, 7 123 681 605, 4 957 339 862, 854 462 070, 3 188 774 179,
3 317 701 700, 5 853 744 121, 7 657 746 574, 325 902 326, 6 801 852 381, 4 943 955 587,
5 279 260 061, 9 574 764 296, 5 718 208 827, 325 902 326, 5 364 733 346, 10 078 344 535,
3 230 641 052, 9 651 118 875, 2 453 237 606, 7 061 103 837, 5 853 744 121, 1 123 759 675,
8 263 781 520, 8 677 774 150, 5 410 172 999, 3 230 641 052, 6 495 678 124, 10 619 632 508,
3 267 211 364, 5 718 208 827, 5 705 870 597, 3 116 927 858, 8 997 086 152, 1 193 340 762,
2 240 718 689, 988 101 827, 8 841 825 481, 7 354 163 795, 7 930 791 608, 144 995 288,
4 594 489 726, 10 334 347 023, 9 953 075 239, 5 410 172 999, 854 462 070, 8 500 386 174,
144 995 288, 3 358 401 938, 1 048 390 117, 3 106 462 717, 5 812 308 154, 2 245 667 888,
632 745 968, 2 010 848 990, 8 444 897 345, 494 238 476, 2 697 838 167, 10 067 292 272,
1 599 544 013, 8 300 952 157, 8 298 254 579, 3 702 610 692, 3 230 641 052, 2 826 961 710,
4 634 311 073, 10 073 868 017, 5 853 744 121, 1 123 759 675, 6 243 001 278, 9 790 984 769,
7 123 681 605, 3 317 701 700, 7 595 812 428, 9 953 075 239, 7 061 103 837, 532 366 792,
4 132 323 499, 3 828 812 904, 390 113 298, 8 824 017 865, 8 677 774 150, 146 675 116, 75 633 548,
9 868 654 492, 3 828 812 904, 7 657 746 574, 325 902 326, 5 079 380 379, 8 406 571 873,
390 113 298, 1 532 337 430, 5 718 208 827, 325 902 326, 632 745 968, 2 010 848 990, 8 444 897 345,
494 238 476, 3 793 008 030, 10 067 292 272, 1 599 544 013, 3 729 366 807, 8 388 070 774,
7 123 681 605, 4 957 339 862, 854 462 070, 3 188 774 179, 3 317 701 700, 5 853 744 121,
7 270 663 960, 2 360 053 725, 2 138 500 761, 2 879 111 763, 8 500 386 174, 9 745 089 678,
4 957 339 862, 2 360 053 725, 9 790 984 769, 7 123 681 605, 3 317 701 700, 7 595 812 428,
1 811 196 615, 5 980 512 470, 2 973 094 056, 3 740 872 486, 10 334 347 023, 1 811 196 615,
5 980 512 470, 8 500 386 174, 7 270 663 960, 9 567 005 779, 3 317 701 700, 3 116 927 858,
7 061 103 837, 532 366 792, 4 132 323 499, 3 828 812 904, 390 113 298, 3 474 650 247,
4 763 588 374, 8 863 444 413, 5 119 528 440, 7 657 746 574, 6 900 059 215, 5 980 512 470,
5 980 512 470, 9 790 984 769, 6 947 517 739, 4 102 961 260, 7 865 602 013, 3 116 927 858,
10 067 292 272, 1 599 544 013, 9 655 074 275, 3 106 462 717, 6 770 477 007, 8 500 386 174,
9 745 089 678, 4 957 339 862, 2 360 053 725, 7 930 791 608, 7 456 014 596, 7 799 562 454,

```
5 718 208 827, 1 659 035 689, 3 882 688 232, 728 378 312, 4 758 674 079, 1 962 045 227,
4 891 168 048, 75 633 548, 6 243 001 278, 6 714 242 794, 5 410 172 999, 5 853 744 121,
255 835 867, 3 955 550 344, 1 792 417 495, 8 127 731 103, 1 200 764 133, 10 067 292 272,
1 599 544 013, 5 443 864 623, 9 745 089 678, 6 947 517 739, 5 443 864 623, 10 322 936 822,
5 380 312 185, 8 801 974 590, 6 900 059 215, 9 574 764 296, 1 792 417 495, 9 588 293 221,
481 374 873, 3 828 812 904, 9 253 212 916, 7 354 163 795, 9 657 650 439, 7 457 995 059,
4 102 961 260, 7 865 602 013, 10 078 344 535, 5 196 733 899, 6 714 242 794, 5 410 172 999,
5 853 744 121, 255 835 867, 3 955 550 344, 1 792 417 495, 8 127 731 103, 1 200 764 133,
10 067 292 272, 1 599 544 013, 5 443 864 623, 9 745 089 678, 6 947 517 739, 5 443 864 623,
10 908 590 807, 2 948 593 242, 4 991 458 112, 3 882 688 232, 10 241 643 857, 7 639 868 313,
3 828 812 904, 9 253 212 916, 2 453 237 606, 4 940 117 279, 8 801 974 590, 2 531 174 014,
4 957 339 862, 8 969 357 150, 8 677 774 150, 8 997 086 152, 1 962 045 227, 1 300 061 741,
9 558 491 159, 5 853 744 121, 1 198 597 571, 1 091 052 264, 5 853 744 121, 3 818 626 831,
3 882 688 232, 728 378 312, 4 758 674 079, 5 853 744 121, 7 657 746 574, 692 406 110,
1 792 417 495, 9 588 293 221, 481 374 873, 3 828 812 904, 9 253 212 916, 10 067 292 272}
```

In[34]:=
```
N[Entropy[2, cryptCodeBinList]]
```
.. энтропия

Out[34]=
```
7.41514
```

8. Расшифровать полученный шифртекст и вывести его в виде строки.

In[35]:=
```
msgCodeBinList = {};
Do[
оператор цикла
 AppendTo[msgCodeBinList, PowerMod[cryptCodeBinList[[i]], secretKey, n]],
 добавить в конец к                степень по модулю
 {i, 1, Length[cryptCodeBinList]}]
        длина
msgCode1List = IntegerPart[msgCodeBinList / 10 000];
                целая часть
msgCode2List = Mod[msgCodeBinList, 10 000];
                остаток от деления
msgCodeList = {};
Do[
оператор цикла
 AppendTo[msgCodeList, msgCode1List[[i]]];
 добавить в конец к
 AppendTo[msgCodeList, msgCode2List[[i]]],
 добавить в конец к
 {i, 1, Length[msgCodeBinList]}]
        длина
Do[If[msgCodeList[[i]] ≥ 2000 && msgCodeList[[i]] < 3000, msgCodeList[[i]] -= 2000],
··· условный оператор
  {i, 1, Length[msgCodeList]}];
         длина
FromCharacterCode[msgCodeList]
символ по его коду
```

Out[42]=
из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить гипотетическую модель потенциального нарушителя [57]:

- квалификация нарушителя может быть на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выберет наиболее слабое звено в защите.

В частности, для банковских АСОИ можно выделить следующие преднамеренные угрозы:

- несанкционированный доступ посторонних лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
- ознакомление банковских служащих с информацией, к которой они не должны иметь доступ;
- несанкционированное копирование программ и данных;
- кража магнитных носителей, содержащих конфиденциальную информацию;
- кража распечатанных банковских документов;
- умышленное уничтожение информации;
- несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;
- фальсификация сообщений, передаваемых по каналам связи;
- отказ от авторства сообщения, переданного по каналам связи;
- отказ от факта получения информации;
- навязывание ранее переданного сообщения;

текст снова совпал с исходным

9. Ввести следующие изменения в Text-N и создать модифицированные строки:

text1– убрать точку в Text-N; (убрана точка в “нарушитель выберет наиболее слабое звено в

защите.”)
text2 – добавить пробел в Text-N; (добавлен пробел перед “из” в самом начале текста)
text3 – поменять местами две расположенные рядом (разные) буквы в Text-N. (“из” заменено на “зи” в самом начале текста)

In[43]:=
```
text1 = "из возможности
    возникновения наиболее опасной ситуации, обусловленной действиями нарушителя,
    можно составить гипотетическую модель потенциального нарушителя  [57]:
• квалификация нарушителя может быть на уровне разработчика данной системы;
• нарушителем может быть как постороннее лицо, так и законный пользователь системы;
• нарушителю известна информация о принципах работы системы;
• нарушитель выберет наиболее слабое звено в защите
\tВ частности,
    для банковских АСОИ можно выделить следующие преднамеренные угрозы:
• несанкционированный доступ посторонних лиц,
    не принадлежащих к числу банковских служащих,
    и ознакомление с хранимой конфиденциальной информацией;
• ознакомление банковских служащих с информацией,
    к которой они не должны иметь доступ;
• несанкционированное копирование программ и данных;
• кража магнитных носителей, содержащих конфиденциальную информацию;
• кража распечатанных банковских документов;
• умышленное уничтожение информации;
• несанкционированная модификация банковскими служащими финансовых документов,
    отчетности и баз данных;
• фальсификация сообщений, передаваемых по каналам связи;
• отказ от авторства сообщения, переданного по каналам связи;
• отказ от факта получения информации;
• навязывание ранее переданного сообщения;
."
text2 = " из возможности возникновения
    наиболее опасной ситуации, обусловленной действиями нарушителя,
    можно составить гипотетическую модель потенциального нарушителя  [57]:
• квалификация нарушителя может быть на уровне разработчика данной системы;
• нарушителем может быть как постороннее лицо, так и законный пользователь системы;
• нарушителю известна информация о принципах работы системы;
• нарушитель выберет наиболее слабое звено в защите.
\tВ частности, для банковских АСОИ можно выделить следующие преднамеренные угрозы:
• несанкционированный доступ посторонних лиц,
    не принадлежащих к числу банковских служащих,
    и ознакомление с хранимой конфиденциальной информацией;
• ознакомление банковских служащих с информацией,
    к которой они не должны иметь доступ;
• несанкционированное копирование программ и данных;
• кража магнитных носителей, содержащих конфиденциальную информацию;
• кража распечатанных банковских документов;
• умышленное уничтожение информации;
• несанкционированная модификация банковскими служащими финансовых документов,
    отчетности и баз данных;
• фальсификация сообщений, передаваемых по каналам связи;
• отказ от авторства сообщения, переданного по каналам связи;
• отказ от факта получения информации;
• навязывание ранее переданного сообщения;
."
text3 = "зи возможности возникновения
```

```
    наиболее опасной ситуации, обусловленной действиями нарушителя,
    можно составить гипотетическую модель потенциального нарушителя  [57]:
• квалификация нарушителя может быть на уровне разработчика данной системы;
• нарушителем может быть как постороннее лицо, так и законный пользователь системы;
• нарушителю известна информация о принципах работы системы;
• нарушитель выберет наиболее слабое звено в защите.
\tВ частности, для банковских АСОИ можно выделить следующие преднамеренные угрозы:
• несанкционированный доступ посторонних лиц,
    не принадлежащих к числу банковских служащих,
    и ознакомление с хранимой конфиденциальной информацией;
• ознакомление банковских служащих с информацией,
    к которой они не должны иметь доступ;
• несанкционированное копирование программ и данных;
• кража магнитных носителей, содержащих конфиденциальную информацию;
• кража распечатанных банковских документов;
• умышленное уничтожение информации;
• несанкционированная модификация банковскими служащими финансовых документов,
    отчетности и баз данных;
• фальсификация сообщений, передаваемых по каналам связи;
• отказ от авторства сообщения, переданного по каналам связи;
• отказ от факта получения информации;
• навязывание ранее переданного сообщения;
•"
```

Out[43]=

```
из возможности возникновения наиболее опасной ситуации, обусловленной действиями
  нарушителя, можно составить гипотетическую модель потенциального нарушителя  [57]:
• квалификация нарушителя может быть на уровне разработчика данной системы;
• нарушителем может быть как постороннее лицо, так и законный пользователь системы;
• нарушителю известна информация о принципах работы системы;
• нарушитель выберет наиболее слабое звено в защите
    В частности, для банковских
  АСОИ можно выделить следующие преднамеренные угрозы:
• несанкционированный доступ посторонних лиц, не принадлежащих к числу
  банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
• ознакомление банковских служащих с информацией,
  к которой они не должны иметь доступ;
• несанкционированное копирование программ и данных;
• кража магнитных носителей, содержащих конфиденциальную информацию;
• кража распечатанных банковских документов;
• умышленное уничтожение информации;
• несанкционированная модификация банковскими
  служащими финансовых документов, отчетности и баз данных;
• фальсификация сообщений, передаваемых по каналам связи;
• отказ от авторства сообщения, переданного по каналам связи;
• отказ от факта получения информации;
• навязывание ранее переданного сообщения;
•
```

Out[44]= из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить гипотетическую модель потенциального нарушителя [57]:

- квалификация нарушителя может быть на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выберет наиболее слабое звено в защите.

В частности, для банковских АСОИ можно выделить следующие преднамеренные угрозы:

- несанкционированный доступ посторонних лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
- ознакомление банковских служащих с информацией, к которой они не должны иметь доступ;
- несанкционированное копирование программ и данных;
- кража магнитных носителей, содержащих конфиденциальную информацию;
- кража распечатанных банковских документов;
- умышленное уничтожение информации;
- несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;
- фальсификация сообщений, передаваемых по каналам связи;
- отказ от авторства сообщения, переданного по каналам связи;
- отказ от факта получения информации;
- навязывание ранее переданного сообщения;
-

Out[45]= зи возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить гипотетическую модель потенциального нарушителя [57]:

- квалификация нарушителя может быть на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выберет наиболее слабое звено в защите.

В частности, для банковских АСОИ можно выделить следующие преднамеренные угрозы:

- несанкционированный доступ посторонних лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
- ознакомление банковских служащих с информацией, к которой они не должны иметь доступ;
- несанкционированное копирование программ и данных;
- кража магнитных носителей, содержащих конфиденциальную информацию;
- кража распечатанных банковских документов;
- умышленное уничтожение информации;
- несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;
- фальсификация сообщений, передаваемых по каналам связи;
- отказ от авторства сообщения, переданного по каналам связи;
- отказ от факта получения информации;
- навязывание ранее переданного сообщения;
-

10. Найти расстояние Дамерау-Левенштейна (DLD) - минимальное количество операций вставки одного символа, удаления одного символа и замены одного символа на другой, необходимых для превращения одной строки в другую- (DamerauLevenshteinDistance[,]) между строкой Text-N и строками text1, text2, text3.

In[46]:=
```
DamerauLevenshteinDistance[msgText, text1]
DamerauLevenshteinDistance[msgText, text2]
DamerauLevenshteinDistance[msgText, text3]
```
расстояние Дамерау–Левенштейна

Out[46]= 1

Out[47]= 1

Out[48]= 1

	text1	text2	text3
DLD	1	1	1

11. Найти расстояние Дамерау-Левенштейна (DamerauLevenshteinDistance[,]) между значениями хэш-функций Hash[] строки Text-N и значениями хэш-функций строк text1, text2, text3.

In[49]:=
```
hashMsg = Hash[msgText]
hash1 = Hash[text1]
hash2 = Hash[text2]
hash3 = Hash[text3]
```
хэш

Out[49]= 3 434 179 239 112 544 549

Out[50]= 4 195 450 690 102 429 656

Out[51]= 6 068 181 285 907 090 055

Out[52]= 6 770 281 966 054 523 455

In[53]:=
```
DamerauLevenshteinDistance[ToString[hashMsg], ToString[hash1]]
DamerauLevenshteinDistance[ToString[hashMsg], ToString[hash2]]
DamerauLevenshteinDistance[ToString[hashMsg], ToString[hash3]]
```
расстояние Дамерау–Левенштейна | преобразовать в строку | преобразовать в строк

Out[53]= 16

Out[54]= 16

Out[55]= 16

	Hash [text1]	Hash[text2]	Hash[text3]
DLD	16	16	16

12. Определить расстояние ДЛ между значениями хэш-функций строк Text-N и text1 для алгоритмов хэширования, приведенных в таблице.

In[56]:=
```
DamerauLevenshteinDistance[msgText, text1]
DamerauLevenshteinDistance[
 ToString[Hash[msgText, "CRC32"]], ToString[Hash[text1, "CRC32"]]]
DamerauLevenshteinDistance[ToString[Hash[msgText, "MD5"]],
 ToString[Hash[text1, "MD5"]]]
DamerauLevenshteinDistance[ToString[Hash[msgText, "SHA"]],
 ToString[Hash[text1, "SHA"]]]
DamerauLevenshteinDistance[ToString[Hash[msgText, "SHA256"]],
 ToString[Hash[text1, "SHA256"]]]
DamerauLevenshteinDistance[ToString[Hash[msgText, "SHA384"]],
 ToString[Hash[text1, "SHA384"]]]
DamerauLevenshteinDistance[ToString[Hash[msgText, "SHA512"]],
 ToString[Hash[text1, "SHA512"]]]
```

Out[56]= 1

Out[57]= 8

Out[58]= 31

Out[59]= 37

Out[60]= 64

Out[61]= 94

Out[62]= 123

«Hash»		“DamerauLevenshteinDistance[]”
«Исходный текст без хэширования»		1
«CRC32»	«32-bit cyclic redundancy check»	8
«MD5»	«128-bit MD5 code»	31
«SHA»	«160 bit SHA-1 code»	37
«SHA256»	«256-bit SHA code»	64
«SHA384»	«384-bit SHA code»	94
«SHA512»	«512 bit SHA code»	123

13. Преобразовать свою фамилию и имя в числовой код m (а->1, ..я->32), получить криптограмму с зашифровав m на секретном ключе ks. Рассмотреть два варианта: разбиение m на максимальное число элементов и разбиение (или его отсутствие) m на минимально возможное число элементов, при этом допускается изменение параметров RSA.

In[63]:=
```
msgText = "нечаевалександр";
msgList = Characters[msgText];
          символы
msgCodeMinList = {};
Do[
оператор цикла
 AppendTo[msgCodeMinList, ToCharacterCode[msgList[[i]]] - 1071],
 добавить в конец к      код символа
 {i, 1, StringLength[msgText]}]
        длина строки
msgCodeMinList = Flatten[msgCodeMinList]
                 уплостить
```

Out[67]= {14, 6, 24, 1, 6, 3, 1, 12, 6, 11, 18, 1, 14, 5, 17}

In[68]:=
```
msgCodeMax = FromDigits[Flatten[Table[
             число по ря··· уплостить таблица значений
    PadLeft[IntegerDigits[msgCodeMinList[[i]]], 2], {i, 1, Length[msgCodeMinList]}]]]
    заполни··· цифры целого числа                  длина
```

Out[68]= 140 624 010 603 011 206 111 801 140 517

In[69]:=
```
SeedRandom[9]
инициализация генератора псевдослучайных чисел
RandomPrime[{Sqrt[100^11], Sqrt[100^11] * 10}, 2]
случайное про··· квадратный кор··· квадратный корень
```

Out[70]= {892 665 323 731, 350 261 647 993}

In[72]:=
```
rsaParamsModule[892 665 323 731, 350 261 647 993]
```

```
N = 312 666 427 396 224 911 421 883

Open key = 95 459 891 171 862 768 459 367

Secret key = 52 592 236 725 673 796 713 063
```

In[73]:=
```
nLong =312 666 427 396 224 911 421 883
openKeyLong = 95 459 891 171 862 768 459 367
secretKeyLong = 52 592 236 725 673 796 713 063
```

Out[73]= 312 666 427 396 224 911 421 883

Out[74]= 95 459 891 171 862 768 459 367

Out[75]= 52 592 236 725 673 796 713 063

In[76]:=
```
cryptCodeMinList = {};
Do[
 AppendTo[
  cryptCodeMinList,
  PowerMod[msgCodeMinList[[i]], secretKeyLong, nLong]],
 {i, 1, Length[msgCodeMinList]}]
cryptCodeMinList
```

Out[78]= {284 036 494 274 362 473 938 354, 307 281 251 204 475 574 122 078, 153 689 229 189 268 633 099 523, 1, 307 281 251 204 475 574 122 078, 270 660 851 830 313 279 062 996, 1, 262 878 728 072 002 346 760 832, 307 281 251 204 475 574 122 078, 76 231 550 698 414 174 608 432, 140 718 830 989 352 764 622 586, 1, 284 036 494 274 362 473 938 354, 220 075 525 491 359 665 049 090, 41 757 106 341 312 926 443 971}

In[79]:=
```
cryptCodeMax = PowerMod[msgCodeMax, secretKeyLong, nLong]
```

Out[79]= 148 180 842 981 928 364 868 754

14. Расшифровать два варианта криптограммы с на ключе ko и получить m.

In[80]:=
```
msgCodeMinList = {};
Do[
 AppendTo[
  msgCodeMinList,
  PowerMod[cryptCodeMinList[[i]], openKeyLong, nLong]],
 {i, 1, Length[cryptCodeMinList]}]
msgCodeMinList
```

Out[82]= {14, 6, 24, 1, 6, 3, 1, 12, 6, 11, 18, 1, 14, 5, 17}

In[83]:=
```
FromCharacterCode[msgCodeMinList + 1071]
```

Out[83]= нечаевалександр

15. Преобразовать строку хеш-кода сообщения m в последовательность (список) чисел при минимальном возможном числе элементов шифрования, определить длину этого списка и

подготовить два новых списка для шифр текста и восстановленного (расшифрованного) хеш-кода. Номер варианта хэш-функции Nmod5+1:

1	2	3	4	5
MD5	SHA	SHA256	SHA384	SHA512

In[100]:=
```
Mod[9, 5] + 1
```
остаток от делен

Out[100]= 5

In[101]:=
```
msgHash = Hash[msgText, "SHA512"]
```
хэш

Out[101]= 7 875 979 193 393 863 308 227 631 599 416 933 095 861 694 969 233 288 379 306 358 295 766 183 110 494 ⁘ 090 600 942 247 980 782 102 979 770 389 385 718 170 144 093 406 556 392 107 184 048 137 449 719 320 ⁘ 477

In[102]:=
```
msgText
```

Out[102]= нечаевалександр

In[103]:=
```
msgHashList = IntegerDigits[msgHash]
```
цифры целого числа
```
Length[msgHashList]
```
длина

Out[103]= {7, 8, 7, 5, 9, 7, 9, 1, 9, 3, 3, 9, 3, 8, 6, 3, 3, 0, 8, 2, 2, 7, 6, 3, 1, 5, 9, 9, 4, 1, 6, 9, 3, 3, 0, 9, 5, 8, 6, 1, 6, 9, 4, 9, 6, 9, 2, 3, 3, 2, 8, 8, 3, 7, 9, 3, 0, 6, 3, 5, 8, 2, 9, 5, 7, 6, 6, 1, 8, 3, 1, 1, 0, 4, 9, 4, 0, 9, 0, 6, 0, 0, 9, 4, 2, 2, 4, 7, 9, 8, 0, 7, 8, 2, 1, 0, 2, 9, 7, 9, 7, 7, 0, 3, 8, 9, 3, 8, 5, 7, 1, 8, 1, 7, 0, 1, 4, 4, 0, 9, 3, 4, 0, 6, 5, 5, 6, 3, 9, 2, 1, 0, 7, 1, 8, 4, 0, 4, 8, 1, 3, 7, 4, 4, 9, 7, 1, 9, 3, 2, 0, 4, 7, 7}

Out[104]= 154

In[105]:=
```
msgHashList = PadLeft[msgHashList, 120];
```
заполнить слева
```
msgHashList = Partition[msgHashList, 20];
```
разбиение на блоки
```
Do[
```
оператор цикла
```
 msgHashList[[i]] = FromDigits[msgHashList[[i]]],
```
число по ряду цифр
```
 {i, 1, Length[msgHashList]}]
```
длина
```
msgHashList
```

Out[108]= {9 586 169 496 923 328 837, 93 063 582 957 661 831 104, 94 090 600 942 247 980 782, 10 297 977 038 938 571 817, 1 440 934 065 563 921 071, 84 048 137 449 719 320 477}

In[109]:=
```
Length[msgHashList]
```
длина

Out[109]= 6

In[110]:=
```
cryptHashList = Table[0, {i, 6}]
                таблица значений
hashFromCryptList = Table[0, {i, 6}]
                    таблица значений
```

Out[110]= {0, 0, 0, 0, 0, 0}

Out[111]= {0, 0, 0, 0, 0, 0}

16. Провести операцию шифрования хеш-кода на ключе ks и зафиксировать результат.

In[112]:=
```
Do[
оператор цикла
 cryptHashList[[i]] = PowerMod[msgHashList[[i]], secretKeyLong, nLong],
                      степень по модулю
 {i, 1, Length[msgHashList]}]
       длина
cryptHashList
```

Out[113]= {228 521 289 628 184 251 809 137, 256 576 452 706 588 166 126 073, 148 385 130 429 247 225 322 315, 285 221 705 069 416 225 963 642, 205 438 112 397 489 605 939 098, 65 101 774 570 586 301 535 574}

17. Провести операцию расшифрования хеш-кода на ключе ko и зафиксировать результат.

In[114]:=
```
Do[
оператор цикла
 hashFromCryptList[[i]] = PowerMod[cryptHashList[[i]], openKeyLong, nLong],
                          степень по модулю
 {i, 1, Length[cryptHashList]}]
       длина
hashFromCryptList
```

Out[115]= {9 586 169 496 923 328 837, 93 063 582 957 661 831 104, 94 090 600 942 247 980 782, 10 297 977 038 938 571 817, 1 440 934 065 563 921 071, 84 048 137 449 719 320 477}

18. Сравнить результат, полученный в п. 17 с исходным хэш-кодом п.15.

In[116]:=
```
msgHashList
hashFromCryptList
HammingDistance[msgHashList, hashFromCryptList]
расстояние Хэмминга
```

Out[116]= {9 586 169 496 923 328 837, 93 063 582 957 661 831 104, 94 090 600 942 247 980 782, 10 297 977 038 938 571 817, 1 440 934 065 563 921 071, 84 048 137 449 719 320 477}

Out[117]= {9 586 169 496 923 328 837, 93 063 582 957 661 831 104, 94 090 600 942 247 980 782, 10 297 977 038 938 571 817, 1 440 934 065 563 921 071, 84 048 137 449 719 320 477}

Out[118]= 0

In[119]:=
```
Do[
оператор цикла
 If[msgHashList[[i]] == hashFromCryptList[[i]],
 условный оператор
  Print["совпадают"],
  печатать
  Print["не совпадают"]; Break[]],
  печатать                прервать цикл
 {i, 1, Length[msgHashList]}]
        длина
```

```
совпадают
совпадают
совпадают
совпадают
совпадают
совпадают
```

Во всех случаях совпадение