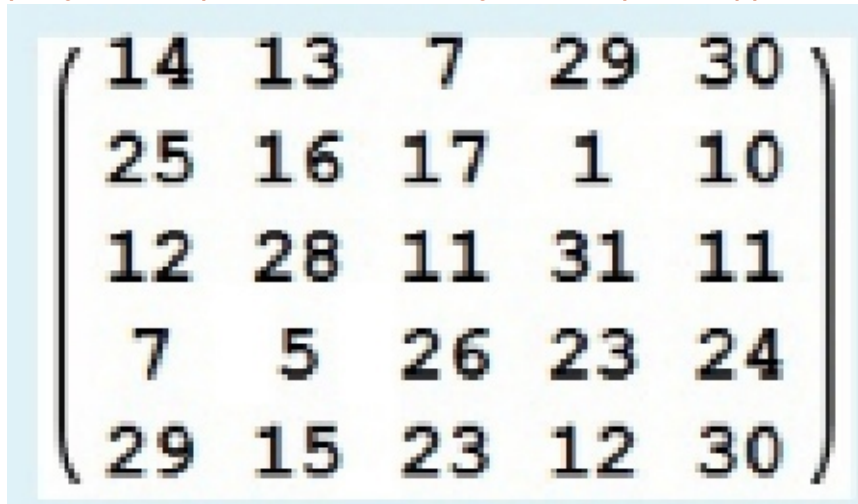


КМ1

1) Расшифровать текст: text1, зашифрованный методом простой перестановки. Ввести первые 15 символов расшифрованного текста в поле ввода. Ответ: сыгранонаславу

```
text1 =
  "соысг лреаднноинйаксилрапвиучввыоппулситниетпервеыкпруасштаилтиесмьегнаярорсеттатлиохсоьпуолз\
  овжаилтсьтоедниднапл";
divs = Divisors[StringLength[text1]] (*список чисел, на которые делится длина текста*)
simpleReorderDecrypt[text_, dimension_] := (
  matrix = Partition[Characters[text], dimension];
  res = Table[matrix[[All, i]], {i, 1, dimension}];
  StringJoin[Flatten[res]]
)
(*здесь получаем перебор всех возможных расшифровок:*)
res1 = Table[{divs[[i]], simpleReorderDecrypt[text1, divs[[i]]}], {i, 1, Length[divs]}]
(*так как ответ под цифрой 2 корректен, то тут надо написать [2,2]:*)
StringTake[res1[[2, 2]], {1, 15}] (*15, потому что нужны первые 15 символов*)
```

2) Расшифровать текст: text2, зашифрованный методом Хилла на ключе, приведенном на рисунке. Определить число букв “м” в расшифрованном тексте. Ответ: 6



14	13	7	29	30
25	16	17	1	10
12	28	11	31	11
7	5	26	23	24
29	15	23	12	30

```
text2 =
  "ршфэеаазупътгшйкатюэчианггышщопюубкшгшвухыэшуямунпхубишьвишьивмцпюсеэюыбамьрютхаууяхыпгца\
  фюфчишшькоеазхаясьцяктуьфнелыощнпфингиэтмьпжэдээдрябщюцехъьцссльбтгюцэспчйцзууфэужды\
  тюхмэмзэкфйхцжъсщйюлкщзчсъяфзрпоййкбцлячювждюцышьгвяузпздчфщюгъйтщбпйагкрьютзбсмхъ\
  цфъяоепживаиыьвяълыупртв";
```

```
decryptMatrix = Inverse[
$$\begin{pmatrix} 14 & 13 & 7 & 29 & 30 \\ 25 & 16 & 17 & 1 & 10 \\ 12 & 28 & 11 & 31 & 11 \\ 7 & 5 & 26 & 23 & 24 \\ 29 & 15 & 23 & 12 & 30 \end{pmatrix}, \text{Modulus} \rightarrow 32];$$

```

```
crypteFiveGrams = Partition[ToCharacterCode[text2] - 1071, 5];
decryptedFiveGrams =
  Table[Mod[Dot[decryptMatrix, crypteFiveGrams[[i]]], 32, 1], {i, 1, Length[crypteFiveGrams]}];
Count[Characters[FromCharacterCode[Flatten[decryptedFiveGrams] + 1071]], "м"]
```

3) Текст фжляцрфлжбгъяцъцир зашифрован с помощью афинной системы подстановок Цезаря с параметрами: $a=23$ $b=24$. Расшифруйте текст и введите результат(строку)в поле ввода. Ответ: двестидевьяностотри

```
afineDeCipher[text_, keya_, keyb_] := FromCharacterCode[
  Mod[Mod[ToCharacterCode[text] - keyb - 1072, 32] * PowerMod[keya, -1, 32], 32] + 1072];
afineDeCipher["фжляцрфлжбгъяцъцир", 23, 24] (*23 (keyA) и 24 (keyB) даны в условии*)
```

4) Расшифровать текст text4, зашифрованный на базовой таблице Вижинера и ключе из таблицы, приведенной на рисунке. Определить число букв "о" в расшифрованном тексте.
 Ответ: 133

N	Ключевое слово	N	Ключевое слово
1	аутентификация	7	сообщение
2	источник	8	идентификатор
3	коммуникации	9	конструкция
4	верификация	10	пользователь
5	целостность	11	протокол
6	теледоступ	12	параметр

text4 =

```
"дюзаошшухэщгэулоютядцхцмкяфашюуъъдхкжцтгтгюбуньоачтьхэыьаекслтфуяомуьбхштггтяхэтьвьошлдцов :
цхольтяшкннапекшуарэаьтыюбъапхцкткоэоыкхэвптхтшуэаьэьрцърэныкяэыбгоьбйююцбчоцпй :
еяьончысыкэуиглыгшхкчэртфъьщрхтшлбывцяоофбхытььюуюаефцаъхптгшхкчэуцркыряозыкртьш :
еоььбпчтщытнвбуатштуэзачычйртюдцъохырящюлзшртмьррауякфцфэбавъэшфэкъцупюяраышжюб :
шагркъудюхсцхлдшгъшкщлъятьчжюбшаубъшшвышааоофбхавцфьэзшгхумпшяццрщъвъхьббпьюхтфкюр :
ьэъхьлопиштяфотпыоэцыоуфйаасшсюзэштткэляюеьбньцвсуыкрявуэуооэцэоэбуудюхеяьбшузхядква :
юцбоийяфуюэйзшкюлахчбютшлцрщъььцчфышачыййэщюнпелцршеяфбхэаьйуньнэанаытртоыцфябашрлщайк :
ьвпууцщпюяраышьььбрщтяжьпършаюшехпещчпкшуароэцыоущюауосццчюмухцнатъчяьуьщюаднцсчтьдй :
эьудаощтэщуамъакойтпыгытшуамьдтшгшызогъфяпчозохцъпрюарчнюющяьбкнкщтчъчутпсбцкьушпбют :
хлбпчвкзъсньюыцготшщбчофохццчбкяоорюдънхштгхяюртайгтпектэпщуччогртяэфыцубъоэчэьбютшщяэб :
эрэсцвзогьловлхчбьояэчышчуцбъьшщаяжтряхриуышывущчыжшушхашаажышщъяьккышаашжшщэээвьншвы :
юешэлфашюььпюяраышэщярбшущъцьюеороррямядббоцчсбвоьщэтяььбццюаьдюнцлцрытшььнпвцяцфьэп :
эцэцийьвбагшхкчэуийяшчыюбмогчяьйапыхкхтвбсккччраштшуярыожпэшуэндкынъэфшвушццчбкзъхьп :
ьльбцъьоэьцежхцчъхьепсщъхрщпщуюхютказэзуякоосфтуэухцвбюпнреяуьмьвпэюлбшыаыпаряпняцц :
шввйууроцчяьцььофъщчяэпюяраышшуьгщгнфтнфацяьяьтошыгакшппявьнунъяззеютщъоабьцэыссьок :
хлвццяшььмвфудэхоэчв";
```

```
keys4 = {"аутентификация", "источник", "коммуникации", "верификация", "целостность", "теледоступ",
"сообщение", "идентификатор", "конструкция", "пользователь", "протокол", "параметр"};
```

(*таблица Вижинера это перебор всех возможных смещений алфавита (например абв,бва,ваб):*)

```
tableVG = Table[RotateLeft[CharacterRange["a", "я"], i], {i, 0, 31}];
```

```
deViziner[plaintext2_, key2_, table_] := (
```

```
text1 = Characters[plaintext2];
```

```
code1 = ToCharacterCode[key2] - 1071;
```

```
dct = {};
```

```
Do[AppendTo[dct, Position[table[[code1[Mod[i - 1, Length[code1]] + 1], All], text1[[i]]][1, 1]],
{i, 1, Length[text1]}];
```

```
FromCharacterCode[dct + 1071]
```

```
)
```

```
res4 = Table[{keys4[[i]], deViziner[text4, keys4[[i]], tableVG]}, {i, 1, Length[keys4]}];
```

```
Count[Characters[res4[[11, 2]], "o"]
```

5) Текст эюышлхкзлызкюехэюкшлэюышлх зашифрован с помощью системы Цезаря. Провести расшифрование и ввести ответ в виде трехзначного десятичного числа в поле ввода. Ответ: 989

```
text5 = "эюышлхкзлызкюехэюкшлэюышлх";
caesarDeCipher[plaintext_, key_] :=
  FromCharacterCode[Mod[ToCharacterCode[plaintext] - 1072 - key, 32] + 1072]
(*перебор всех возможных расшифровок, смотрим где выглядит корректно:*)
Table[{i, caesarDeCipher[text5, i]}, {i, 1, 33}]
```

6) Расшифровать текст text6, зашифрованный на ключе из таблицы, приведенной на рисунке. В поле ввода ввести строку из 11 символов, которые расположены начиная с 35 позиции в расшифрованном тексте. Ответ: ачкубанкнот

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

```
keys6 = {"барокамера", "ватерлиния", "галантерея", "двухтомник", "жилплощадь", "заповедник",
  "кавалерист", "легкоатлет", "магнитофон", "нормировка", "радиолампа", "стекловата"};
text6 =
  "нзвктвннкюрааааеоденкткрнанатосгктжерлвушежирибнолулкаесппрбакзосыеиетиааабузучблеоаеазии\
  тивбртнотлодоуштноиознднлвмпмлнчссоеууабкеотлврыауаноеърнксеркисанлриааоахрюзудпоеев\
  ппирхнунттрибывокрррптсезндтеупрпповсоеидиакусивппрйпсаылныыевщчэтнчхеганоаеов";
simpleReorderKeyDecrypt[text_, passphrase_] := (
  CrTable =
    Transpose[Partition[Characters[text], StringLength[text] / StringLength[passphrase]]];
  key = Ordering[Ordering[Characters[passphrase]]];
  DecrTable = Table[CrTable[[i, key]], {i, StringLength[text] / StringLength[passphrase]};
  StringJoin[DecrTable]);
res6 = Table[{keys6[[i]], simpleReorderKeyDecrypt[text6, keys6[[i]]}], {i, 1, Length[keys6]};
(*начиная с 35го, 11 символов:*)
StringTake[res6[[6, 2]], {35, 35 + 10}]
```

7) Найти ключ смещения, с помощью которого зашифрован текст: text. Шифрование выполнено методом Цезаря с ключевым словом: “вариконд”. Ввести ключ смещения в поле ввода. Ответ: 8

```
text7 =
  "кшбфчъшгвифэъошгонъшгршыишьшчяшкнимшичньвоынънбвирнбшциэъэсэоэдбнбновиовгинъшчозкныжнщтчгов\
  ефгршрвкъубшюэовэкногкнебэиошкшбфцъшгвифэъожъбжыноъгешъшивяшгенишвошмвошибгйшювъшефд\
  н";
caesarDeCipherWord[text_, keya_, keyb_] := (
  a1 = CharacterRange["а", "я"];
  a2 = RotateRight[Join[Characters[keya], Complement[a1, Characters[keya]]], keyb];
  StringReplace[text, Apply[Rule, Partition[Riffle[a2, a1], 2], 1]]
)
(*перебор всех возможных расшифровок,
смотрим где выглядит корректно и пишем НОМЕР, а не саму строку:*)
Table[{i, caesarDeCipherWord[text7, "вариконд", i]}, {i, 1, 32}] // TableForm
```

КМ2

1) По заданной двоичной последовательности 1011100110101010100110111 определить коэффициентобратной связи РСЛОС. Вводить коэффициенты, начиная со старших разрядов. Ответ: 100100011

Null (*по идее такой задачи не будет, иначе грустно...*)

```
bm[s_] := (Lol = 0; fol = 1; diff = 0; Clear[x]; f = 1; L = 0;
g = CoefficientList[f, {x}];
Do[If[Mod[Sum[g[[i]] s[[j - 1 - L + i]], 2] == s[[j]], diff = diff + 1, Lne = Max[j - L, L];
fne = PolynomialMod[xLne-L f + xLne-Lol-diff-1 fol, 2];
If[Lne ≠ L, fol = f; Lol = L; L = Lne; diff = 0, diff = diff + 1];
f = fne; g = CoefficientList[f, {x}]]];
If[j == Length[s], Print["j=", j, ", L=", L, ", f=", f], {j, Length[s]}]]
bm[ToExpression[StringSplit["1011100110101010100110111", ""]]]
```

2) Регистр сдвига с линейными обратными связями имеет характеристический многочлен $x^{11} + x^9 + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$. Начальное состояние РСЛОС определяется числом 516. Определить состояние РСЛОС в десятичной форме на 1833-ом такте работы. Ответ: 1643

```
LFSR[data0_, numb0_] := Module[{data = data0, count = numb0},
(*тут важно перечислить все S до последней степени X (не включая последнюю)
например у нас полином 11ой степени, значит последнее будет s10:*)
  {s10, s9, s8, s7, s6, s5, s4, s3, s2, s1, s0} = data;
  outLstLFSR = {};
(*здесь тоже про полином не забываем*)
  Do[{s10, s9, s8, s7, s6, s5, s4, s3, s2, s1, s0} =
    {Mod[s9 + s7 + s6 + s5 + s3 + s2 + s1 + s0, 2], s10, s9, s8, s7, s6, s5, s4, s3, s2, s1};
    If[i == count,
      Print[i, " ", {s10, s9, s8, s7, s6, s5, s4, s3, s2, s1, s0}]],
    {i, count}];]
count4 = 1833;
data4 = PadLeft[IntegerDigits[516, 2], 11];
(*11 потому что полином 11ой степени, а 516 дано в условии*)
LFSR[data4, count4] (*еще не ответ*)
1833 {1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1}
Null FromDigits[{1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1}, 2] (*ВОТ ответ*)
```

3) Зашифровать строку открытого текста, состоящую из 30 символов(букв и пробелов):"калиостро же доказал что она нн", шифром RC4, в котором S - блок представлен в виде набора 256 случайных целых чисел из диапазона 0-255. Начальное значение генератора случайных чисел равно:1147. Определить сумму кодов шифртекста. Ответ: 31061

```
Null text = "калиостро же доказал что она нн";
SeedRandom[1147];
s = RandomInteger[{0, 255}, 256];
i = 0; j = 0;
genNum := (i = Mod[i + 1, 256];
j = Mod[j + s[[i + 1]], 256];
{s[[i + 1]], s[[j + 1]]} = {s[[j + 1]], s[[i + 1]]};
t = Mod[s[[i + 1]] + s[[j + 1]], 256];
K = s[[t + 1]]);
nums = ToCharacterCode[text];
codes = Table[genNum, {k, Length[nums]}];
Total[BitXor[nums, codes]]
```

4) Расшифровать текст:

”тпшггщиыбпфнщлцюзййэдмжбагтцкнххпсбуммсэплховеиччбьфсызоюзд”. Стартовое значение генератора случайных чисел, формирующего двоичную последовательность ключа, равно 592. Определить сумму кодов символов в расшифрованном тексте. Ответ: 64948.

```
Null ctText = "тпшггщиыбпфнщлцюзййэдмжбагтцкнххпсбуммсэплховеиччбьфсызоюзд";
SeedRandom[592];
(*длина*5, потому что каждая буква шифруется с помощью 5 бит:*)
codes = RandomInteger[{0, 1}, StringLength[ctText] * 5];
nums = Flatten[Table[PadLeft[IntegerDigits[ToCharacterCode[ctText][[i]] - 1072, 2], 5],
  {i, 1, StringLength[ctText]}]];
fiveDigitsList = Partition[BitXor[nums, codes], 5];
UnCoded = Table[FromDigits[fiveDigitsList[[i], 2] + 1072, {i, 1, Length[fiveDigitsList]}];
Total[UnCoded]
```

5) Последовательность чисел {129, 200, 115, 131, 183, 126, 121, 197, 30, 99, 216, 113} является результатом шифрования строки текста шифром RC4, в котором S-блок представлен виде набора 256 случайных целых чисел из диапазона 0 - 255. Начальное значение генератора случайных чисел равно 5415. Расшифровать текст и ввести в поле ввода любое одно слово. Ответ: sat

```
Null (*отличается от задания 3) только добавлением FromCharacterCode[] в последней строчке:*)
sumbCodes = {129, 200, 115, 131, 183, 126, 121, 197, 30, 99, 216, 113};
SeedRandom[5415];
s = RandomInteger[{0, 255}, 256];
i = 0; j = 0;
genNum := (i = Mod[i + 1, 256];
j = Mod[j + s[[i + 1]], 256];
{s[[i + 1]], s[[j + 1]]} = {s[[j + 1]], s[[i + 1]]};
t = Mod[s[[i + 1]] + s[[j + 1]], 256];
K = s[[t + 1]]);
codes = Table[genNum, {k, Length[sumbCodes]}];
FromCharacterCode[BitXor[sumbCodes, codes], "ISOLatinCyrillic"]
```

6) Зашифровать текст:

”огуэтогосделатьпочемуспросилкарабасбарабастолькодлятогочтобы”. Стартовое значение генератора случайных чисел, формирующего двоичную последовательность ключа, равно 484. Определить число дырок “0000” в двоичной последовательности шифртекста. Ответ: 11

```
Null ctText = "огуэтогосделатьпочемуспросилкарабасбарабастолькодлятогочтобы";
SeedRandom[484];
codes = RandomInteger[{0, 1}, StringLength[ctText] * 5];
nums = Flatten[Table[PadLeft[IntegerDigits[ToCharacterCode[ctText][[i]] - 1072, 2], 5],
  {i, 1, StringLength[ctText]}]];
(*после BitXor мы можем получить цифру 0 или 1, но если взять по таблице ASCII,
то 0 это 48 ой символ, а 1 - 49 йй, поэтому тут и + 48 : *)
fiveDigitsList = StringCount[FromCharacterCode[BitXor[nums, codes] + 48], "0000"]
```

КМЗ

1) Найти секретный ключ Ks асимметричной криптосистемы RSA, если открытый ключ Ko - код результата шифрования символа “у” с ключом 12 в системе шифрования Цезаря, а

числа P и Q, составляющие модуль N - ближайшие простые числа, превышающие величину энтропии криптосистемы IDEA . Ответ: 8287

```
Null letter = "y";
shift = 12;
criptEntrop = 128; (*для Gost=256,IDEA=128,DES=56;
RC4=40-2048,AES=128,192,258*)
code = Mod[shift + ToCharacterCode[letter] - 1072, 32] + 1072;
P = NextPrime[criptEntrop];
Q = NextPrime[criptEntrop, 2];
private = PowerMod[code, -1, EulerPhi[P * Q]]
```

2) Сумма контракта подписана двумя участниками сделки: 2587475708. Модуль для ЭЦП равен 2857185293. Значение хэш - функции ("CRC32") общего третьего ключа равно 1909677311. Файл со значениями ключей находится в папке: K33 модуль 3/OpenKey/keys.dat. Определить сумму контракта. Ответ: 412485

```
Null module = 2 857 185 293;
hash = 1 909 677 311;
key1 = 2 587 475 708;
key3 =
  Select[ReadList["C:\\Users\\TSLA\\Downloads\\keys2020.dat"], Hash[#, "CRC32"] == hash &][[1]];
PowerMod[key1, key3, module]
```

3) Провести операцию умножения двух байтов a={80} и b={e7} по правилам, специфицированным в шифре AES: с приведением результата по модулю полинома $x^8+x^4+x^3+x+1$. Пример ввода ответа:{ff} Ответ: {d1}

```
Null a = 16^80;
b = 16^e7;
polM = x^8 + x^4 + x^3 + x + 1;
polA = Expand[FromDigits[IntegerDigits[a, 2], x]];
polB = Expand[FromDigits[IntegerDigits[b, 2], x]];
BaseForm[
  FromDigits[Reverse[Mod[CoefficientList[PolynomialRemainder[polA * polB, polM, x], x], 2], 2], 16]
```


4) Для схемы разделения секрета на основе интерполяционных полиномов Лагранжа (7,14) известны семь долей: K1 = 235; K2 = 2521; K3 = 1544; K6 = 2163; K7 = 50; K10 = 2579; K12 = 3594; Определить значение секрета M, если величина модуля p = 3673. Ответ: 1038

Null (*Мне было проще запомнить вступую:*)

```
Clear[a1, a2, a3, a4, a5, a6, m]
```

```
k1 = 235;
```

```
k2 = 2521;
```

```
k3 = 1544;
```

```
k6 = 2163;
```

```
k7 = 50;
```

```
k10 = 2579;
```

```
k12 = 3594;
```

```
p = 3673;
```

```
(*кол-во уравнений и кол-во параметров равно кол-ву известных k:*)
```

```
Solve[
```

```
a6 * 1^6 + a5 * 1^5 + a4 * 1^4 + a3 * 1^3 + a2 * 1^2 + a1 * 1 + m == k1 && (*x1, потому что k1*)
```

```
a6 * 2^6 + a5 * 2^5 + a4 * 2^4 + a3 * 2^3 + a2 * 2^2 + a1 * 2 + m == k2 && (*x2, потому что k2*)
```

```
a6 * 3^6 + a5 * 3^5 + a4 * 3^4 + a3 * 3^3 + a2 * 3^2 + a1 * 3 + m == k3 && (*x3, потому что k3*)
```

```
a6 * 6^6 + a5 * 6^5 + a4 * 6^4 + a3 * 6^3 + a2 * 6^2 + a1 * 6 + m == k6 && (*x6, потому что k6*)
```

```
a6 * 7^6 + a5 * 7^5 + a4 * 7^4 + a3 * 7^3 + a2 * 7^2 + a1 * 7 + m == k7 && (*x7, потому что k7*)
```

```
a6 * 10^6 + a5 * 10^5 + a4 * 10^4 + a3 * 10^3 + a2 * 10^2 + a1 * 10 + m == k10 &&
```

```
(*x10, потому что k10*)
```

```
a6 * 12^6 + a5 * 12^5 + a4 * 12^4 + a3 * 12^3 + a2 * 12^2 + a1 * 12 + m == k12, (*x12, потому что k12*)
```

```
{a6, a5, a4, a3, a2, a1, m}, Modulus -> p]
```

Null (*но можно решить и по умному:*)

```
p = 3673;
```

```
k = {235, 2521, 1544, 2163, 50, 2579, 3594};
```

```
numsK = {1, 2, 3, 6, 7, 10, 12};
```

```
count = 7;
```

```
powers = Join[Reverse[Table[ToExpression[StringJoin["a", ToString[i]]], {i, 1, count - 1}]], {M}];
```

```
coefs = Map[Expand[FromDigits[powers, #]] &, numsK];
```

```
exps = Table[coefs[[i]] == k[[i]], {i, 1, count}];
```

```
Solve[exps, powers, Modulus -> p][[1, 1]]
```

5) Сообщение:Прилетаю четырнадцатого июля, подписано электронно-цифровой подписью RSA. Модуль системы = 340835287621. Открытый ключ = 41364825743, хэш - функция "CRC32". Определить, какая из приведенных подписей действительна. Ответ: 14cbe295a

Null text = "Прилетаю четырнадцатого июля";

```
mod = 340835287621;
```

```
pubK = 41364825743;
```

```
hash = Hash[text, "CRC32"];
```

```
BaseForm[PowerMod[hash, PowerMod[pubK, -1, EulerPhi[mod]], mod], 16]
```

ПРИКОЛЫ

1) Номер автомобиля зашифрован по схеме шифрования Полига-Хеллмана: {105, 810, 1709, 1089, 906, 105, 810, 810}. Значение функции Эйлера Φ от ключа шифрования равно: 712 Известны также следующие параметры системы: модуль $n=1777$ и диапазон возможных ключей шифрования $[\Phi, 10*\Phi]$. Определить номер автомобиля. Пример ввода ответа: B001AP190

```
n = 1777;
shifr = {105, 810, 1709, 1089, 906, 105, 810, 810};
e = 712;
ee = e * 10 + 1;
While[e < 7121,
If[EulerPhi[e] == 712, Print[e];
Break]; e++];
895
1432
1790
2148

d = PowerMod[895, -1, EulerPhi[n]] (*подставляем по очереди числа, пока не получим внятно*)
deshifr = {};
Do[AppendTo[deshifr, Mod[shifr[[i]]^d, n]], {i, 1, Length[shifr]}];
FromCharacterCode[Flatten[deshifr]]
```

2) Номер автомобиля зашифрован по схеме шифрования Полига-Хеллмана: {1971, 1595, 1042, 1516, 1009, 760, 1516, 1516}. Значение функции Эйлера Φ от ключа шифрования равно: 1716. ЗИ Практика (основной файл).nb 21 Известны также следующие параметры системы: модуль $n=2311$ и диапазон возможных ключей шифрования $[\Phi, 10*\Phi]$. Определить номер автомобиля. Пример ввода ответа: B001AP190. //номер из 8 символов

```
c = {1971, 1595, 1042, 1516, 1009, 760, 1516, 1516};
n = 2311;
eu = 1716;
k = {};
d = {};
eu2 = EulerPhi[n]
Do[If[EulerPhi[i] == eu, AppendTo[k, i];
AppendTo[d, PowerMod[i, -1, eu2]]], {i, eu, n}]
k
d
Mod[k * d, eu2]
Do[Print[FromCharacterCode[PowerMod[c, d[[j]], n]]], {j, Length[k]}]
```