Лабораторная работа №3 “Криптосистема Хилла”

In[2]:=
```
alfa = CharacterRange["а", "я"]
```
Out[2]=
```
{а, б, в, г, д, е, ж, з, и, й, к, л, м, н,
 о, п, р, с, т, у, ф, х, ц, ч, ш, щ, ъ, ы, ь, э, ю, я}
```

1. Сформировать матрицу преобразования для реализации криптосистемы Хилла размером 2x2: {{3,3},{2,5}}.

In[1]:=
```
matrix = {{3, 3}, {2, 5}};
```

2. Рассчитать детерминант матрицы (Det[]) и проверить, являются ли делители (Divisors[]) числа 32 (длина русского алфавита) и значение детерминанта взаимно простыми числами (GCD[]).

In[3]:=
```
detM = Det[matrix]
```
Out[3]=
```
9
```

In[4]:=
```
Map[Function[{a}, GCD[a, detM] == 1], Divisors[32]]
```
Out[4]=
```
{True, True, True, True, True, True}
```

3. Найти матрицу обратного преобразования: Inverse[*,Modulus->32] и выполнить проверку, перемножив (Dot[]) прямую и обратную матрицы по модулю 32.

In[5]:=
```
matrixInv = Inverse[matrix, Modulus → 32]
```
Out[5]=
```
{{29, 21}, {14, 11}}
```

In[6]:=
```
Mod[#, 32] & /@ Dot[matrix, matrixInv]
```
Out[6]=
```
{{1, 0}, {0, 1}}
```

4. Подготовить текст «прилетаювосьмого» для шифрования: заменить каждую букву на её числовой эквивалент и разбить полученный список на биграммы.

In[10]:=
```
openText = "прилетаювосьмого";
openTextSim = Position[alfa, #][[1, 1]] & /@ Characters[openText];
openTextSimBi = Partition[openTextSim, 2]
```
Out[12]=
```
{{16, 17}, {9, 12}, {6, 19}, {1, 31}, {3, 15}, {18, 29}, {13, 15}, {4, 15}}
```

5. Провести шифрование первой биграммы: перемножить матрицу прямого преобразования на вектор (в данном случае первую биграмму) по модулю 32 со смещением 1 (Mod[*,32,1]).

In[13]:=
```
Mod[Dot[matrix, openTextSimBi[[1]]], 32, 1]
```
Out[13]=
```
{3, 21}
```

6. Зашифровать весь текст и преобразовать его из числовых эквивалентов в строку.

In[16]:=
```
cypTextBy = Mod[Dot[matrix, #], 32, 1] & /@ openTextSimBi;
cypText = StringJoin[alfa[[#]] & /@ Flatten[cypTextBy]]
```
Out[17]=
```
вфюнккяьхрмфудшт
```

7. Шифртекст, полученный в п.6 подготовить к дешифрованию: заменить каждую букву на

её числовой эквивалент и разбить полученный список на биграммы.

In[18]:=
```
cypTextSim = Position[alfa, #][[1, 1]] & /@ Characters[cypText];
cypTextSimBy = Partition[cypTextSim, 2]
```

Out[19]=
```
{{3, 21}, {31, 14}, {11, 11}, {32, 29}, {22, 17}, {13, 21}, {20, 5}, {25, 19}}
```

8. Провести дешифрование первой биграммы: перемножить матрицу обратного преобразования на вектор (в данном случае первую биграмму) по модулю 32 со смещением 1 (Mod[*,32,1]).

In[20]:=
```
Mod[Dot[matrixInv, cypTextSimBy[[1]]], 32, 1]
```

Out[20]=
```
{16, 17}
```

9. Расшифровать весь текст и преобразовать его из числовых эквивалентов в строку.

In[23]:=
```
decTextBy = Mod[Dot[matrixInv, #], 32, 1] & /@ cypTextSimBy
decText = StringJoin[alfa[[#]] & /@ Flatten[decTextBy]]
```

Out[23]=
```
{{16, 17}, {9, 12}, {6, 19}, {1, 31}, {3, 15}, {18, 29}, {13, 15}, {4, 15}}
```

Out[24]=
```
прилетаювосьмого
```

10. Задать начальное состояние генератора случайных чисел равное номеру по списку в группе, получить 16 случайных целых чисел из интервала [1,32] и сформировать матрицу размером 4x4.

11. Выполнить п. 2 и п.3, и если проверки не выполняются - сформировать новый набор случайных чисел.

In[25]:=
```
MatrixDim = 4;
SeedRandom[20]
generated = False;
matrixCyp = {};
While[! generated ,
 matrixCyp =
  Partition[RandomInteger[{1, 32}, MatrixDim * MatrixDim], MatrixDim];
 detM = Det[matrixCyp];
 generated = True;
 Map[Function[{a}, generated = generated && (GCD[a, detM] == 1)], Divisors[32]];
]
matrixCyp
```

Out[26]=
```
RandomGeneratorState[ Method: ExtendedCA
                      State hash: 8 311 514 930 021 384 083 ]
```

Out[30]=
```
{{20, 25, 2, 10}, {10, 27, 27, 12}, {19, 23, 23, 15}, {31, 7, 16, 30}}
```

12. Подготовить открытый текст для шифрования: импортировать файл соответствующий номеру 50 - N и содержащий открытый тест (папка Plaintext; distributives\ импорт открытого текста.nb), удалить пробелы, привести размер текста к величине кратной 4.

In[31]:=
```
openText = "про меня
    сразу забыли в совершенном отчаянии я вышел в коридор и столкнулся с
    уянусомкоторый сказал так и помедлив осведомился не беседовали ли мывчера
    нет сказал я к сожалению не беседовали он пошелдальше и я услышал как в
    конце коридора он задает все тот жестандартный вопрос жиану жиакомо в
    конце концов меня занесло к абсолютникам я попал перед самымначалом
    семинара сотрудники позевывая и осторожно поглаживая уширассаживались в
    малом конференцзале на председательском месте покойносплетя пальцы
    восседал завотделом магистракадемик всея белыя черныя исерыя магии
    многознатец морисиоганнлаврентий пупковзадний иблагосклонно взирал на
    суетящегося докладчика который с двумя неумеловыполненными волосатоухими
    дублями устанавливал на экспозиционном стенденекую машину с седлом и
    педалями похожую на тренажер для страдающихожирением я присел в уголке
    подальше от остальных вытащил блокнот иавторучку и принял заинтересованный
     вид нутес произнес магистракадемик у вас готово да морис иоганнович
    отозвался л седловой готово морисиоганнович тогда может быть приступим
    чтото я не вижу смогулия он в командировке иоганн лаврентьевич сказали из
    зала ах да припоминаю экспоненциальные исследования ага агану хорошо
    сегодня у нас луи иванович сделает небольшое сообщениеотносительно
    некоторых возможных типов машин времени я правильноговорю луи иванович э
    собственно собственно я бы назвал свой доклад такимобразом что а ну вот и
    хорошо вот вы и назовите благодарю вас э назвал бы так осуществимость
    машинывремени для передвижения во временных пространствах
    сконструированных"
openText = StringReplace[openText, {" " → ""}];
openTextLength = Floor[StringLength[openText] / 4] * 4;
openText = StringTake[openText, openTextLength]
```

Out[31]= про меня сразу забыли в совершенном отчаянии я вышел в коридор и столкнулся с уянусомкоторый сказал так и помедлив осведомился не беседовали ли мывчера нет сказал я к сожалению не беседовали он пошелдальше и я услышал как в конце коридора он задает все тот жестандартный вопрос жиану жиакомо в конце концов меня занесло к абсолютникам я попал перед самымначалом семинара сотрудники позевывая и осторожно поглаживая уширассаживались в малом конференцзале на председательском месте покойносплетя пальцы восседал завотделом магистракадемик всея белыя черныя исерыя магии многознатец морисиоганнлаврентий пупковзадний иблагосклонно взирал на суетящегося докладчика который с двумя неумеловыполненными волосатоухими дублями устанавливал на экспозиционном стенденекую машину с седлом и педалями похожую на тренажер для страдающихожирением я присел в уголке подальше от остальных вытащил блокнот иавторучку и принял заинтересованный вид нутес произнес магистракадемик у вас готово да морис иоганнович отозвался л седловой готово морисиоганнович тогда может быть приступим чтото я не вижу смогулия он в командировке иоганн лаврентьевич сказали из зала ах да припоминаю экспоненциальные исследования ага агану хорошо сегодня у нас луи иванович сделает небольшое сообщениеотносительно некоторых возможных типов машин времени я правильноговорю луи иванович э собственно собственно я бы назвал свой доклад такимобразом что а ну вот и хорошо вот вы и назовите благодарю вас э назвал бы так осуществимость машинывремени для передвижения во временных пространствах сконструированных

Out[34]= променясразузабыливсовершенномотчаянииявышелвкоридористолкнулсясуянусомкоторый сказалтакипомедливосведомилсянебеседовалилимывчеранетсказаляксожалениюнебе седовалионпошелдальшеияуслышалкаквконцекоридораонзадаетвсетотжестандартный вопросжианужиакомовконцеконцовменязанеслокабсолютникамяпопалпередсамымнача ломсеминарасотрудникипозевываяиосторожнопоглаживаяуширассаживалисьвмаломко нференцзаленапредседательскомместепокойносплетяпальцывосседалзавотделоммаг истракадемиквсеябелыячерныяисерыямагиимногознатецморисиоганнлаврентийпупко взаднийиблагосклонновзиралнасуетящегосядокладчикакоторыйсдвумянеумеловыпол неннымиволосатоухимидублямиустанавливалнаэкспозиционномстенденекуюмашинусс едломипедалямипохожуюнатренажердлястрадающихожирениемяприселвуголкеподальш еотостальныхвытащилблокнотиавторучкуипринялзаинтересованныйвиднутеспроизне смагистракадемикувасготоводаморисиоганновичотозвалсялседловойготовоморисио ганновичтогдаможетбытьприступимчтотояневижусмогулияонвкомандировкеиоганнла врентьевичсказалииззалаахдаприпоминаюэкспоненциальныеисследованияагааганух орошосегодняунаслуиивановичсделаетнебольшоесообщениеотносительнонекоторыхв озможныхтиповмашинвременияправильноговорюлуиивановичэсобственнособственноя быназвалсвойдокладтакимобразомчтоанувотихорошовотвыиназовитеблагодарювасэн азвалбытакосуществимостьмашинывременидляпередвиженияввременныхпространств ахсконструирован

13. Провести шифрование открытого текста 4-граммами и определить число совпадений 4-грамм в зашифрованном тексте.

In[39]:=
```
openTextSim = Position[alfa, #][[1, 1]] & /@ Characters[openText];
openTextSim4 = Partition[openTextSim, 4];
cryptTextSim4 = Mod[Dot[matrixCyp, #], 32, 1] & /@ openTextSim4;
cryptTex = StringJoin[alfa[[#]] & /@ Flatten[cryptTextSim4]]
```

Out[42]=
```
иытьйнбчдмэнфражкуеюмфкгсэшфмнэхдтрттржпдмръцзнчшбхзсфюжжкошехпнусйгжлюрочйгып
ьухмходнгсмыньямошпфщтосйбэеухйлчгрыкжйрйкоржлбизязжцзомощщшояфэищэьуннлып
эруйжиксяупфуыгжуишраюмречдпявтатыуырюйьшпэнмпыщуъгпнрютщкхйкфбщвомйоэайек
яыъчэтъыьлъгъквххпшгаэндьдтсаьхэвьрмктярзыящяоиеуакщбщндшяыержзкндтшдякъчц
фгхиъхэитзюбрсдэбвфцсюлжшдзиырврккхвамаагцршатэпщхсхмтчцщичфтжиксдпшояювиаш
жушрффничшчръльзкндфбшжсжощоэчуыкюывсжкчкжгхйкэйъъзшжиэнйтвдрбсъунэзлэжтлфх
емьвъйссьсройеаънйзпнхренлфгчркпойэвъуцйэциймтппьшечсэжшжрдцжшпюихвпщяпйеиу
жэжцопдьоьйвхжсопьдсяъцпьеьькрцфмкнффбиярьвщхъцбгэочйгязвяйшпшчевбяшлчхмрл
хпзяднъийжчрфпмлмщвжуумоюбеврчужрктбшдхзлфпьашзжцхоыьчыжяхямпыveъчютшцчэзч
ибъчоъйфызгвхсшъгъйолшмэизълыьифйсолааюйдээфжтфонсгъярохутсацхмдэочьепуишр
кеафьяхкхчцшзюаофтоаиэлрвхпгюяепеимыяаидяпхбоъачаармдйкщесапфклсхеацмсвчуп
фбэалжфзлэюотзмваэупнюочззмябутоцыэдбаоэоштщцвдлздупчйвъщюоруэвпчяшхящэжшж
рдцжшщшемъильсяыовшжъитхгрйькссоозчззяшыюкегктчужюуфощмшктъпшэччщцкррдцжшп
юиэтысдяномчбълмьрбтъзктоыярржкяъцъулмучяфпыонжфигщнюгэебякглсвкзотнхкхзкф
мбуебнаждцсугфвщптеэжжтеарэчыглвкювтшиемкиллкшйегрьяшдфчкпурцфбащкснмнмнрб
чюфывпхцйыюбровзтбтжмщзивлийърефлюлъюцкхаяасжфньъкыгтъяхешщбцкяисъднйцуъдг
йнъядлздфсйюияиыаэйпмулевщыфюамеиъбптянгжпвджущбшошпцтщъющцяэвмщфгебмщцбза
кгафбяъчдвщпмъэжсбкеьэфчэеицпнтжмщщднблпнзсцмвъазлпюритжмщйящгякщлолааэцйщ
лепвлщщмгдьидйкщ
```

14. Расшифровать текст с номером 15+N (Лаб. 4 Crypttext Hill), который был зашифрован в рамках криптосистемы Хилла с ключом:

In[48]:=
```
matrixCyp5 = {{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}};
matrixDeCyp5 = Inverse[matrixCyp5, Modulus → 32];
```

In[50]:=
```
crypText5 =
 "пшееаньирыфуччщюуящчъшымзюгъжкагилуэуюхаезкэхсцпбжмвтбяииылтзккъзновнаозещп↓
    кгцясщфзхюинюзеннйащеикжыынетьггыпэщдьээемджды йпивиынэохжтъмэдгхщжъмевхя↓
    эдыыфъеиарсэйылийюцббагюпзэефухшздхоьшхйбоэйьымймюжфъткгялдпзопдзшцупьиз↓
    ежышатйъйоайццнъхнцсэжэоэьдсрждшйюющнщзтыъкчиофшлайзцояачщгъгчрампйчрйрц↓
    ыдгтзшдзьйгкочжшраниьпетсхгькрнаашсжьлуыфгрурдбюнсэхчфяшщфэюцпауффайаоыъ↓
    вфсщнчиоанфрымйяцфмртзщмйючиковйсъллъвгвзрвлгрузцмдеыэисжтпфцяьцыйъфхар↓
    кывшемхочаьччлхвцмизфэбшуйеаорччэцй"
crypTextSym = Position[alfa, #][[1, 1]] & /@ Characters[crypText5];
crypTextSym5 = Partition[crypTextSym, 5];
decTextSym5 = Mod[Dot[matrixDeCyp5, #], 32, 1] & /@ crypTextSym5;
decText5 = StringJoin[alfa[[#]] & /@ Flatten[decTextSym5]]
```

Out[50]=
```
пшееаньирыфуччщюуящчъшымзюгъжкагилуэуюхаезкэхсцпбжмвтбяииылтзккъзновнаозещпкгц↓
    ясщфзхюинюзеннйащеикжыынетьггыпэщдьээемджды йпивиынэохжтъмэдгхщжъмевхяэдыыф↓
    ъеиарсэйылийюцббагюпзэефухшздхоьшхйбоэйьымймюжфъткгялдпзопдзшцупьизежышатй↓
    ъйоайццнъхнцсэжэоэьдсрждшйюющнщзтыъкчиофшлайзцояачщгъгчрампйчрйрцыдгтзшдзь↓
    йгкочжшраниьпетсхгькрнаашсжьлуыфгрурдбюнсэхчфяшщфэюцпауффайаоыъвфсщнчиоанф↓
    рымйяцфмртзщмйючиковйсъллъвгвзрвлгрузцмдеыэисжтпфцяьцыйъфхаркывшемхочаьчч↓
    лхвцмизфэбшуйеаорччэцй
```

Out[54]=
```
увертывалсяотшучивалсяпросилудерживатьбезнегопозицииберечьпочкиненапрягатьсяив↓
    концеконцовтакникеминеуловленныйвыкатилсяиззданияпривычновзмахнувнераскрыт↓
    ымпропускомпередносомдежурногосержантанадгородомвиселинизкиетучипарилоперв↓
    ыенеуверенныекапличернымизвездочкамирасплывалисьнаасфальтенакинувплащнагол↓
    овуиплечинунанрысцойпобежалвдольшеренгимашинксвоемупежонырнулвнутрьисорвав↓
    сголовыплащбросилегоназаднеесиденьеизбоковогокарманапиджакаонизвлекчернуюк↓
    руглуюпалочкуэтакавста
```