Оглавление

[Криптосистема Хилла 3](#_Toc507745607)

[Пример-шифрование 3](#_Toc507745608)

[Пример-расшифрование 4](#_Toc507745609)

[Расширенный алгоритм Евклида 5](#_Toc507745610)

[Задание 1 7](#_Toc507745611)

[Задание 2 7](#_Toc507745612)

[Задание 3 8](#_Toc507745613)

[Задание 4 8](#_Toc507745614)

[Режимы шифрования 9](#_Toc507745615)

[Задание 5 12](#_Toc507745616)

[Задание 6 12](#_Toc507745617)

[Задание 7 12](#_Toc507745618)

[Задание 8 12](#_Toc507745619)

[Задание 9 13](#_Toc507745620)

[Задание 10 13](#_Toc507745621)

[Задание 11 13](#_Toc507745622)

[Задание 12 13](#_Toc507745623)

[Задание 13 14](#_Toc507745624)

[Задание 14 14](#_Toc507745625)

[Задание 15 14](#_Toc507745626)

[Задание 16 14](#_Toc507745627)

[Задание 17 14](#_Toc507745628)

[Задание 18 15](#_Toc507745629)

[Частотный анализ 16](#_Toc507745630)

[Задание 19 17](#_Toc507745631)

[Пример дешифрации криптограммы 18](#_Toc507745632)

[Варианты к заданию 19 21](#_Toc507745633)

[1 21](#_Toc507745634)

[2 21](#_Toc507745635)

[3 21](#_Toc507745636)

[4 21](#_Toc507745637)

[5 21](#_Toc507745638)

[6 21](#_Toc507745639)

[7 22](#_Toc507745640)

[8 22](#_Toc507745641)

[9 22](#_Toc507745642)

[10 22](#_Toc507745643)

[11 22](#_Toc507745644)

[12 22](#_Toc507745645)

[13 23](#_Toc507745646)

[14 23](#_Toc507745647)

[15 23](#_Toc507745648)

[16 23](#_Toc507745649)

[17 23](#_Toc507745650)

[18 24](#_Toc507745651)

[19 24](#_Toc507745652)

[20 24](#_Toc507745653)

[Литература 25](#_Toc507745654)

# Криптосистема Хилла

Шифр замены. Только замена выполняется не символа на символ, а блока символов на блок символов. Такой шифр называют блочным. Рассмотрим случай, когда блок состоит из двух символов. Идея замены была предложена Хиллом в статьях: L. S. Hill, "Concerning certain linear transformation apparatus of cryptography", American Mathematical Monthly, Volume 38 (1931), 135-154. Lester S. Hill, Cryptography in an Algebraic Alphabet, The American Mathematical Monthly Vol.36, June–July 1929, pp. 306–312.

### Пример-шифрование

Рассмотрим сообщение:

THE GOLD IS BURIED IN ORONO.

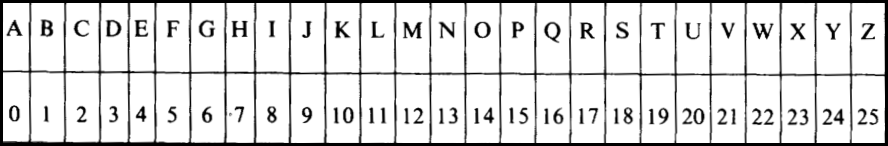
Сформируем блоки по 2 символа:

TH EG OL DI SB UR IE DI NO RO NO.

Т.к. у каждого символа есть свой числовой эквивалент (табл.1), то полученные блоки будут выглядеть так:

19 7 4 6 14 11 3 8 18 1 20 17 8 4 3 8 13 14 17 14 13 14.

Таблица 1



Каждый блок из двух чисел  исходного сообщения преобразуется в блок из двух чисел  зашифрованного сообщения по следующей формуле:



где , , А – матрица размерности 2x2.

Пусть , тогда шифрование первого блока  будет выглядеть так:



где 



Если применить эту формулу ко всем блокам, то получим следующий результат:

6 25 18 2 23 13 21 2 3 9 25 23 4 14 21 2 17 2 1l l8 l7 2.

Или в символьном виде:

GZ SC XN VC DJ ZX EO VC RC LS RC.

### Пример-расшифрование

Расшифрование выполняется по формуле:

,

где  - обратная к матрица по mod 26.

Для матрицы



если определитель



является взаимно простым со значением модуля (в данном случае 26), то

обратную матрицу  можно найти по следующей формуле:



где  - обратное значение по умножению для  по модулю 26.

Для матрицы  обратная по модулю 26 будет матрица

.

Тогда, расшифровка, например, первого зашифрованного блока будет такой:

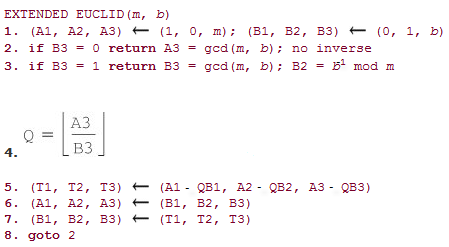
,

где 



### Расширенный алгоритм Евклида

Для поиска обратного значения по умножению применяют расширенный алгоритм Евклида рис.1.

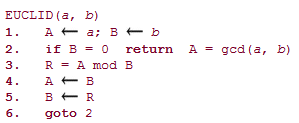
 –

1. – Расширенный алгоритм Евклида [1]

Реализация в Python:

|  |
| --- |
| def findModInverse(a, m):  # Returns the modular inverse of a % m, which is  # the number x such that a\*x % m = 1  if gcd(a, m) != 1:  return None # no mod inverse if a & m aren't relatively prime  # Calculate using the Extended Euclidean Algorithm:  u1, u2, u3 = 1, 0, a  v1, v2, v3 = 0, 1, m  while v3 != 0:  q = u3 // v3 # // is the integer division operator  v1, v2, v3, u1, u2, u3 = (u1 - q \* v1), (u2 - q \* v2), (u3 - q \* v3), v1, v2, v3  return u1 % m |

В приведенном коде используется функция gcd –реализация алгоритма Евклида поиска наибольшего общего делителя двух чисел (рис.2):



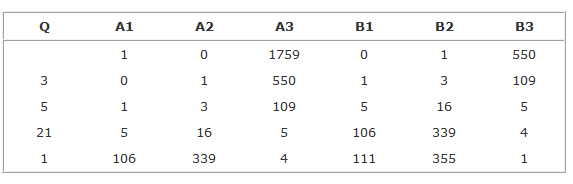
1. – Алгорим Евклида [1]

Реализация в Python:

|  |
| --- |
| def gcd(a, b):  # Return the GCD of a and b using Euclid's Algorithm  while a != 0:  a, b = b % a, a  return b |

## Задание 1

Найти обратное значение по умножению для 550 по mod 1759. В таблице показана пошаговая реализация алгоритма, приведенного на рис.1.



Проверить полученный результат с помощью функции findModInverse. Для этого функции gcd и findModInverse записать в файл utilFunctions.py. После этого импортировать в свою программу функцию findModInverse:

from utilFunctions import findModInverse

Найти обратное для а=141:

a\_inv = findModInverse(a, 256)

## Задание 2

Расшифровать файл im3\_hill\_c\_all.bmp. Ключ – матрица K=[[189 58]

[ 21 151]].

Чтоб сделать код наглядней, можно импортировать функции для чтения и записи данных из файла так:

from read\_write\_file import read\_data\_1byte as read

from read\_write\_file import write\_data\_1byte as write

Тогда, прочитать данные из файла:

c\_data = read('im3\_hill\_c\_all.bmp ')

## Задание 3

Дешифровать png-файл b4\_hill\_c\_all.png. Первые четыре байта в любом png-файле: 137, 80, 78, 71.

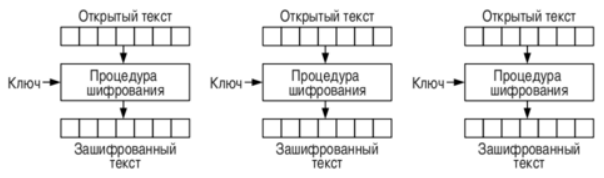
## Задание 4

Дешифровать файл text2\_hill\_c\_all.txt. Известно, что текст в файле начинается со слова Whose.

# Режимы шифрования

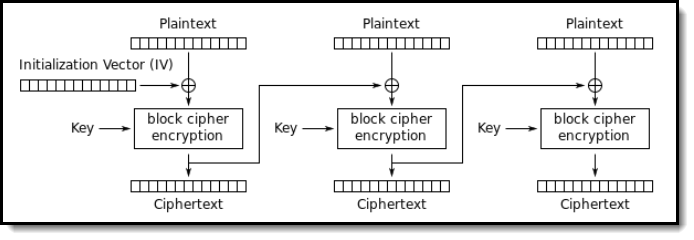
Дополнить нижеприведенные схемы описанием преимуществ и недостатков перечисленных режимов шифрования.

Рассмотренные ранее алгоритмы выполнялись в режиме ECB (рис.3).

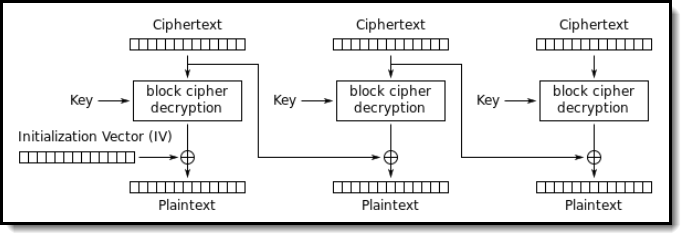


1. – Шифрование в режиме ECB

Режим шифрования CBC (рис.4, 5).

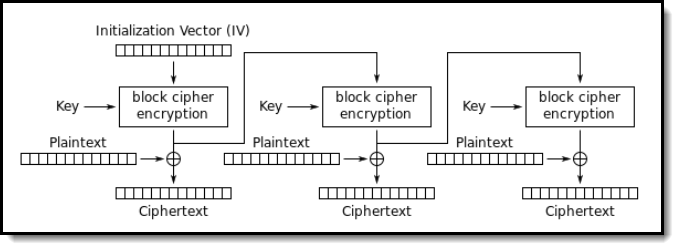


1. – Шифрование в режиме CBC

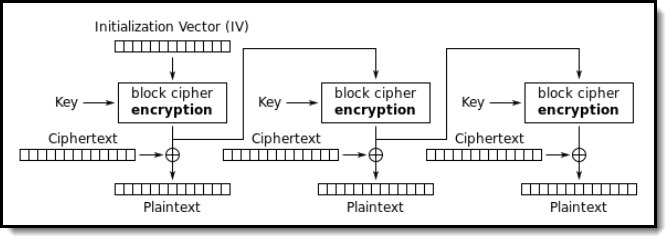


1. – Расшифрование в режиме CBC

Режим шифрования OFB (рис.6, 7).

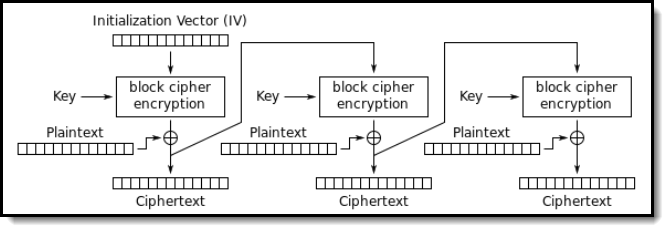


1. – Шифрование в режиме OFB

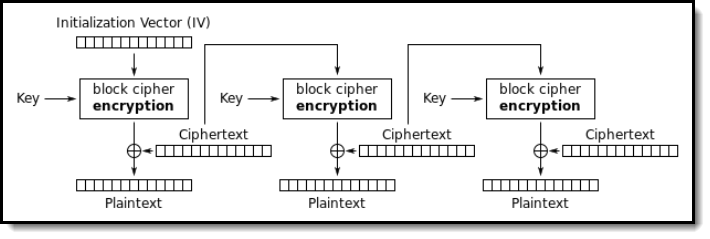


1. – Расшифрование в режиме OFB

Режим шифрования CFB (рис.8, 9).

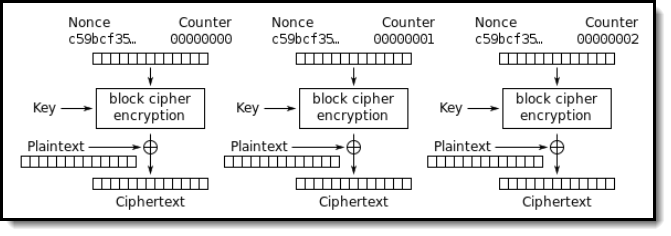


1. – Шифрование в режиме CFB

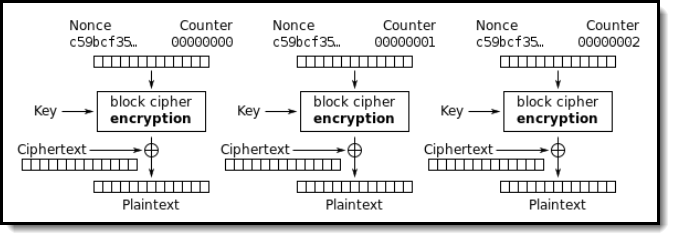


1. – Расшифрование в режиме CFB

Режим шифрования CTR (рис.10, 11).



1. – Шифрование в режиме CTR



1. – Расшифрование в режиме CTR

## Задание 5

Проверьте, что для данных [1, 2, 3, 4] результат шифрования в режиме CBC шифром Цезаря с ключом 3 и вектором инициализации 1 будет [3, 4, 10, 17].

## Задание 6

Расшифровать файл z1\_caesar\_cbc\_c\_all.bmp – зашифрованное шифром Цезаря изображение в формате bmp. Режим шифрования CBC (рис. , ). Ключ равен 223. Вектор инициализации равен 59. Зашифровать в режиме ECB и в режиме CBC, оставив первые 50 байт без изменения. Сравнить полученные изображения.

## Задание 7

Расшифровать файл im8\_caesar\_ofb\_c\_all.bmp – зашифрованное шифром Цезаря изображение в формате bmp. Режим шифрования OFB (рис. , ). Ключ равен 56. Вектор инициализации равен 9. Зашифровать в режиме ECB и в режиме OFB, оставив первые 50 байт без изменения. Сравнить полученные изображения.

## Задание 8

Расшифровать файл z2\_caesar\_cfb\_c\_all.bmp – зашифрованное шифром Цезаря изображение в формате bmp. Режим шифрования CFB (рис. , ). Ключ равен 174. Вектор инициализации равен 9. Зашифровать в режиме ECB и в режиме СFB, оставив первые 50 байт без изменения. Сравнить полученные изображения.

## Задание 9

Расшифровать файл z3\_caesar\_ctr\_c\_all.bmp – зашифрованное шифром Цезаря изображение в формате bmp. Режим шифрования CTR (рис. , ). Ключ равен 223. Вектор инициализации равен 78. Зашифровать в режиме ECB и в режиме CTR, оставив первые 50 байт без изменения. Сравнить полученные изображения.

## Задание 10

Для одного из расшифрованных изображений выполнить следующее: на одном и том же ключе и векторе инициализации зашифровать во всех рассмотренных режимах, включая ECB, оставив первые 50 байт без изменения. Сравнить полученные изображения.

## Задание 11

Расшифровать файл z5\_vigener\_cbc\_c\_all.bmp. Шифр Виженера. Режим CBC. Ключ: MODELING, вектор инициализации: 67. Зашифровать, оставив первые 50 байт без изменения.

## Задание 12

Расшифровать файл im4\_vigener\_ofb\_c\_all.bmp. Шифр Виженера. Режим OFB. Ключ: MODULATOR, вектор инициализации: 217. Зашифровать, оставив первые 50 байт без изменения.

## Задание 13

Расшифровать файл im5\_vigener\_cfb\_c\_all.bmp. Шифр Виженера. Режим CFB. Ключ: MONARCH, вектор инициализации: 172. Зашифровать, оставив первые 50 байт без изменения.

## Задание 14

Расшифровать файл z6\_vigener\_ctr\_c\_all.bmp. Шифр Виженера. Режим CTR. Ключ: MONOLITH, вектор инициализации: 167. Зашифровать, оставив первые 50 байт без изменения.

## Задание 15

Расшифровать файл im15\_affine\_cbc\_c\_all.bmp. Шифр аффинный. Режим CBC. a= 129 b= 107 iv = 243. Зашифровать, оставив первые 50 байт без изменения.

## Задание 16

Расшифровать файл im16\_affine\_ofb\_c\_all.bmp. Шифр аффинный. Режим OFB. a= 233 b= 216 iv = 141. Зашифровать, оставив первые 50 байт без изменения.

## Задание 17

Расшифровать файл im17\_affine\_сfb\_c\_all.bmp. Шифр аффинный. Режим CFB. a= 117 b= 239 iv = 19. Зашифровать, оставив первые 50 байт без изменения.

## Задание 18

Расшифровать файл z4\_affine\_сtr\_c\_all.bmp. Шифр аффинный. Режим CTR. a= 61, b= 18, iv = 92. Зашифровать, оставив первые 50 байт без изменения.

# Частотный анализ

Все естественные языки имеют характерное частотное распределение символов. Например, буква “О” \_ встречается в русском языке чаще других, а буква “Ф” – самая редкая (табл. 2).

Моноалфавитные подстановки обладают важным свойством: они не нарушают частот появления символов, характерных для данного языка. Это позволяет криптоаналитику легко получить открытый текст при помощи частотного анализа. Для этого нужно сопоставить частоты появления символов шифра с вероятностями появления букв используемого алфавита ( в данном случае русского ). После этого наиболее частые символы криптограммы заменяются на наиболее вероятные символы алфавита, остальные замены производятся на основе вероятных слов и знания синтаксических правил используемого языка.

              Таблица 2. Вероятности встречаемости букв русского языка

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Символ | вер\_ть | символ | вер\_ть | символ | вер\_ть |
| Пробел | 0.175 | К | 0.028 | Ч | 0.012 |
| О | 0.089 | М | 0.026 | Й | 0.010 |
| Е | 0.072 | Д | 0.025 | Х | 0.009 |
| А | 0.062 | П | 0.023 | Ж | 0.007 |
| И | 0.062 | У | 0.021 | Ю | 0.006 |
| Н | 0.053 | Я | 0.018 | Ш | 0.006 |
| Т | 0.053 | Ы | 0.016 | Ц | 0.004 |
| С | 0.045 | З | 0.016 | Щ | 0.003 |
| Р | 0.040 | Ь | 0.014 | Э | 0.003 |
| В | 0.038 | Б | 0.014 | Ф | 0.002 |
| Л | 0.035 | Г | 0.013 |  |  |

## Задание 19

Используя частотный анализ, дешифровать криптограмму, зашифрованную методом моноалфавитных подстановок. Напишите отчет о проделанной работе. В отчете необходимо представить: номер варианта, расшифрованный исходный текст, ключ (в данном случае ключом является таблица замен), краткий протокол криптоанализа (см. пример).

## Пример дешифрации криптограммы

Пример дешифрации криптограммы, зашифрованной моноалфавитной подстановкой

Текст криптограммы:

КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙЖТЛЙАСБДНСЙАШЩАСЩЖ

---------------------------------------------------------------------

ЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ

------------------------------

В таблице 3 находятся результаты статистического анализа данной криптограммы. Сюда включены значения частот букв русского языка, а также частоты встречаемости символов для данной криптограммы.

Таблица 3

СТАТИСТИКА

|  |  |  |  |
| --- | --- | --- | --- |
| Криптограмма | | Русский язык | |
| Символ | Частота | Буква | Вероятность |
| А | 0.121 | Пробел | 0.175 |
| Щ | 0.111 | о | 0.090 |
| С | 0.101 | е | 0.072 |
| Й | 0.091 | а | 0.062 |
| Н | 0.081 | и | 0.062 |
| Ш | 0.081 | н | 0.053 |
| Т | 0.071 | т | 0.053 |
| Б | 0.051 | с | 0.045 |
| Р | 0.040 | р | 0.040 |
| Д | 0.040 | в | 0.038 |
| Ж | 0.040 | л | 0.035 |
| и т.д. | | и т.д. | |

Исходя из полученной статистики, сделаем первые замены: “А”-“ ”, “Щ”-“О”.

Результат:

КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙЖТЛЙАСБДНСЙА

-О-----О--- ----------- -- ---- ------------О-О ------- ------

ШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ

-О -О---О ---- О- -О----О--О -------

Обратим внимание на 8-ое и 12-ое слова: “ШЩ” и “ЩШ”. Т.к. мы предположили, что “Щ” заменяет “О” в открытом тексте, то буква “Ш” может быть только буквой “Н” или буквой “Т”. Попробуем сделать замену “Ш”-“Н”.

Можно предположить, что 5-ое слово - оканчивается на “ОГО” и является, стало быть, прилагательным или причастием.

Замена “М”-“Г”.

Слово, следующее за прилагательным или причастием, скорее всего является существительным и оканчивается на “А”. Отсюда следует замена “Й”-“А”.

Теперь имеем следующую картину:

КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙЖТЛЙАСБДНСЙА

-О---АНО--- ----------- НА -А-- --А---------ОГО АНА---А -----А

ШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ

НО -О---О ---- ОН -О--А-О-НО ---НН--

Четвертым словом является предлог “НА”, поэтому следующее слово оканчивается, скорее всего, на букву “Е”.

Заменяем “Б”-“Е”.

Шестое слово имеет вид “АНА---А”. Это очень похоже на слово “АНАЛИЗА”. Заменим “Ж”-“Л”, “Т”-“И”, “Л”-“З”.

Результат:

КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙЖТЛЙАСБДНСЙА

-О---АНО--И -Е-И------- НА -АЗЕ --А-И--И-Е--ОГО АНАЛИЗА -Е---А

ШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ

НО -ОЛ--О Е-ЛИ ОН -О--А-О-НО -ЛИНН--

Словосочетание “НА -АЗЕ” означает, видимо, слова “НА БАЗЕ”, слово “Е-ЛИ” является словом “ЕСЛИ”, а последнее слово криптограммы “-ЛИНН--” похоже на слово “ДЛИННЫЙ”. Сделаем соответствующие замены: “Ь”-“Б”, “Н”-“С”, “Р”-“Д”, “И”-“Ы”, “Г”-“Й”.

Результат:

КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙЖТЛЙАСБДНСЙА

-ОДС-АНО--И ДЕ-И-----С- НА БАЗЕ С-А-ИС-И-ЕС-ОГО АНАЛИЗА -Е-С-А

ШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ

НО -ОЛ--О ЕСЛИ ОН ДОС-А-О-НО ДЛИННЫЙ

Слово “С-А-ИС-И-ЕС-ОГО” (АНАЛИЗА) похоже на слово “СТАТИСТИЧЕСКОГО”. Замены: “С”-“Т”, “О”-“Ч”, “Д”-“К”.

Результат:

КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙЖТЛЙАСБДНСЙА

-ОДСТАНО-КИ ДЕ-И----ТС- НА БАЗЕ СТАТИСТИЧЕСКОГО АНАЛИЗА ТЕКСТА

ШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ

НО ТОЛ-КО ЕСЛИ ОН ДОСТАТОЧНО ДЛИННЫЙ

Последующие замены не вызывают затруднений.

Исходный текст:

ПОДСТАНОВКИ ДЕШИФРУЮТСЯ НА БАЗЕ СТАТИСТИЧЕСКОГО АНАЛИЗА ТЕКСТА НО ТОЛЬКО ЕСЛИ ОН ДОСТАТОЧНО ДЛИННЫЙ

Ключ (таблица замен):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Нормативный  Алфавит ( M ) | А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П |
| Алфавит  Шифрования(E) | Й | Ь | Х | М | Р | Б | - | Л | Т | Г | Д | Ж | - | Ш | Щ | К |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Нормативный  Алфавит (M) | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ы | Ь | Э | Ю | Я | “\_“ |
| Алфавит  Шифрования (E) | П | Н | С | Ф | Ц | - | - | О | У | - | И | Е | - | Ю | Ы | А |

Прочерки в таблице соответствуют буквам, ни разу не встретившимся в исходном тексте криптограммы.

## Варианты к заданию 19

### 1

ЫЛЖФСХХНЙМЕЙФЙЭТДСМДСХАЫЛЦХЖМЫЕЭЫДЖЧРСЙЫЬМДМФЙДЙМБНАТЬЗЙТСМЦ

ЯЙХОМКСБЦЕСЫХЦМБМЬФДСШМТЭЯЖШМЫЦТХ ЖМЫБЙФДЖЧРЖЬМФЙДЖМЭЫЙЬХХЖЬ

МЫДЦТОВЬРСУСМТЦЗДЖУСМЦДЖГУТЙХХЖЬМТЙЫЦУМЗЦФЦАЖМСВЬРХНЙМБСТТНМ

ХЖМЗФЭАЦУМИЙФЙАЭМАЖФФСЫМБМЫБЦЙГМДФЖЫХЦГМЫМЦФЖХКЙБНУМЮЭЮЖГДЙМ

ЕФЙЗЫЛЖБТЬТСМЫЦИЦГМЬФДЭЧМДЖФЛСХЭ

### 2

ЕСЙЮЯУФРЛХСЧВСХ ЬФРТСЖБРЧРУЭРХФЯФВЩБВЬЖУРСП БЖУРМХСЖБТ ЬЖУРП

БЖУ БЖУРУРЧВХФЙЮЩБВЬЖУРПХЬЯБЖУР БЛСЖУ БГВРЗХФЖФ БРТЙУ ЬЭРЩК

ЙСПРУРПБЖАСЙСЗРЯУВЬЭРИФЖЩКМСЖРИУЙФВСЗРУРАБЖЬЧЙСЗБВЬЭРПЙЫВЗРЙ

ГТУРПСВСХЬФРЗСАЗФЙУРНВУРТСЖБРКЖФЙУРЧВХСУВЮ

### 3

ХБЮЖХЛЖЮЩЫБХЛЖДЛЖЗХПНЫЯЛЖЫЖЗПДЯЛГХЛЦЫПЫШИЛЮЛВХФБХЖСЛЩЫБХЗСЛЫ

ЯЛЦРБДЛЖДЧЫПНЫГГДЛГЫМЫШДЛХЛЖЮЩЫЗСЛЦЫЭЛЩЫБХЛЖХВЮЛЭГХЫЗЫЛЩЫБДЛ

ГЫБЫШАДЫЛПХЭЛЩПИШДЯЛДГХЛЕПХЧЩХЛЖИГИБХЛГДЖЛЧЛАГЮШИЛАДЗДПИУЛЖЫ

ЖЗПХЛМЮЗХБХЛГДЛЗХВЛГЫЛДАХЭХБДЖСЛГЮЛАХПЗЮГДАЛГЮЛЖЗЮНАДЧ

### 4

ЩДГЕФШСЫЙЯСКХЖЩЯСЛДЕГЬЮЬЯЬКСЛДЕГЬЫЬЕЬАСФСЬЫЯТАТЯС ЬСКЯЬЮТХСК

ЬЮЕДХДГГФВЬЮСЬЫТУЭДЯОГЬПСЮГДИГЬКЭОРСГТЕУАСДЩЬСЫЙЯСГТСЕДАВЬКЭ

ОСЫЬЩТЭСТЭЯТКГЙПСМДЯДГЙПСВТЦЭТГСКСЫДЯЙХФС ЕЬЕДМУХФСЫДЕДЭСКСЫ

ДЯЙХС ДЕЬХСЫЯФКЭТЮИФПСБДХЛЖЩЬХСФСТЯХТМТХФСИ ТЩТСЕТЫЬЭЙСЫДГЮД

ГЖЭЬ

### 5

ЫПВЮДЕХЧГДЗУЧРТПЧУЬЫГФДЧЭЫГДНГЙЧГДРДНГЖРСЙГФДНУЩЧФДПБЖГЧГБЮД

ЫГУОРЫУДБПДНЗУНОГЩРДТГНГЧПБЮДВЖПДЬПТГДЩХДУУДОУЖРДБЬГЧРДНЗУНО

ХДЗДЖРЙРЫУДРДЕУНЩПЧЗРРДЛГНКПЗГЛРЗГЧРДБДЫУМДПДТГТРСДЖПДЗУЧРТР

СДЖГАЫГСДРСДКПЧПБДЕХЧДБЧРЙТПЩДЫРНПТДРДКЧЭЕПТДВЖПЕХДЩХДЧМОРДЩ

ПКЧРДЭЧПЗРЖЮДУКПДЫГЙРЩДОУЖБТРЩДЭСПЩ

### 6

ПЙХБГХЫХЮХЭМНХБЙЩЦЮЩПНЕЗБНЙЦСЙЙГПЗБГЮНБЬХГКЮХБПХЦЗБГЩДСБМЗРЗ

ТБЛКШНБЛЗМЗШВМКДНБЫЮХТДХГЗДНБЫЩПЙХТМХПМЩАЩБЩЛН ЩТЗБЖБЬЗЙГЩБЙ

ЫЮЗЭНПЗУБЙХЛЖБТХИЙГПНГХШВМЩБШНБЦЮЗЙНПКБЙГЗЮНММКХБЙСЫЩПКХБГЗЮ

ХШЦНБЦЩГЩЮКХБДКБГЗЦБПКЙЩЦЩБФХМНДБНШНБГЩШВЦЩБЩЮХЩШБТЮХПМЩЙГНБ

ЫЮНТЗХГБНДБЫЮХШХЙГВБПБМЗЭН БАШЗРЗ

### 7

ИЬЭЛЬЕТЦЫЭГМВЬЫГТЫЖЦЭЗЦЫЭГВЭИЖЫЭГКГВКЧЫЭГЦЫГЯГЯЫРЩМЧЭГЗМЯТВЯ

МЭВТБГЦЕЬЕТВЕФОЭЭГЯЫЖЦЭЦКЭГЛЫЬЫЖЙГКЫЕЦЦГТВЫКВГЯГЩЕЦЛЬЕЮВГЧЫЖ

ЖЭГКГЯЭТЙГЩЭЦЙГЦЕЛЕЦМЦЭГНЫЬЫЩЫЛГЫНЖЕАЕЖТБГПЬБ ЕЦКЭСГЫЬМХКБГК

ГТВМЛЫСГЛЫИУВГИЫГСЫТВЫЯЫДГЛЬКЛЫСГЛЫСЕЦЩКЬЫЯГИЬЫЛЖБВКБСКГКГНЬ

МПУСКГАМВЛЕСКГПЫЬЫЩЕВУЧГЖМЗЦКЛЫЯ

### 8

СМФВЦОКЮОПНЭЛЭЯАВЛПИВЛВШДЙПДЕРУЯЭПРЮВОЦЦЭОПФТЮЭФСПСПЧВКАТФСП

ФВКОФСПДИЛЭМДЙЭКЭПЯЛРАТВПДИЛТЙТПЯПЦСФПЕДЗЮАРЕЭКСПЕЛОФТВПЙКЭЧ

ЦТВПЖЭБСПВКВЩПСНПЙВЛУСЦТПЛЭМЗВКОКСЮХПЮСЦВЩПБВКХЫПЛРЖВЩПЛЭЮУС

ЛОКЮОПЦЭЛЭЮАЭКДПВШДПАВЖВЦСВПУСЛСЦЭПРЙВКСЖСЙЭКЭЮХПЕЛСМЛЭЖЦТЩП

ИКВЮЯПФВКЯДШДПЕВЮЖЭЦДШДПЗЦЭПРШЭЮЭК

### 9

АМЩПЭИЭКСАЩСЮКЩЭТОСАЭМЭОПВОСТБМРБМУИБСАЩАБПБСКСФМОРЩЕСАЭМЭЮЭ

ВБКЛУЕСАЭМКШЕСАЩФСАМНТШТСОРПЩТСЫИЩИСЯБАПБИБГГШЕСВМУКЩЕСФПУГГ

ШЕСАЭМЭОПЩВСЮСАЩВЩЮУКЛЭЕЮНСФКЭМЖХСГЭЦИЭПБКВУСРФЭСВМОЬВБТУСАМ

ЩФБХИСВЭМЩЮУГСЩГБСАЭМЭМЭЯБПБСКСЩФГЩСТРГЩКЭГУЭСТБМРБМУИБСЮЬБП

БСЙЭИВОСАЩПЭИЭПБСКРПНФШКБНЮЖСКСКШКЭЮВУ

### 10

ЕГЙЙЧЫШШКЧЯЬДНЧРДЯЙНЭРДЮКЯШЧЯДФЧЦНЯБЭШЫНДЫЯЭЯФШЭПДЩЯЛБЧ ГНРЧШДЫЩЯЙНЭРОЯДАЛЧЙНШКЩЯЬДНЧРЫФЯУЧЕЧЛЧШОЯДРДЯПЭЕЭУМЭЛЯШГБЕДФЧЕЯЭЗЯЭЬДУГШДДЯБЭ НЭЛЭПЭЯУШЫЯЛЭЯЛНЭЕШДМЯДЯБЫНШДЮСЯБЭРМЭЛГЫЯШГВГЯМГШЮЧРЫЕДЫЯЗКЛГРГЯБЭРШГЯШГЕЭУСЯМНЭЯЬУГРЯУЧШЧПЯМНЭЯБДЙОФГЯМНЭЯПГАЧН

### 11

ЩАРДЕАЭЦЩМЧРВНЦЛДСХ ГДЦОДЗПЖДЦОЦУЩМСПРЩФЦЛЧАЩОЩЧЦОДЗЧРВЧЦДЦТЦЩЙЖПКЭОДТМВЦМЛЩСЗЧЖЦРДЦГПБХЯПЧЦБЧРГПЦЙДСН ГДЦХЦЩГРДЦЯПСДЖЦБЗПАОЩЗРЭФЦГДЖЧРАДЗВЦЧЕЧУЩАРЩЦПЛЦБЩЖХЯДЧЛЭФЦИСДЦГРПУДЦПЛЧЖДЦОМЧУАДЦМПЖВРЩЧЦРДЦРЧУЩЦОЖПТРПЧЦРПГЩУАДЦРЧЦБЧЗЧЯПСЭОДЖЦЩРЦЧЧЦЙЧКЦЩМЩЙЧРРЩУЩЦХЯДМСПТ

### 12

ЙФЧЗРДХВЭРЖРЖЕДМВДПЭЫДХВУЕЙШЯПЖЕДМЖДПВЭ ВРДЕВТЖШЗДКЫЬЖЕЗДШЩНЬМВДПЫ ЫЩДФЫЬШНД ЫФДЮЖЭДВ ДЮЖЭНДЭ ЖМВПЗЕЭЙДЭЗЕЦМЫЫДВКЕЖЮРВДВКЩЖ ЗЕВЭЦДПДКЫЕНСД НЮНДРВ ВЩЖЙД ЙЬЫЕВДХВШЯФЖЕЖЭЦДЩВЭЕЖДЗДХВЭ ЫХЫММВДВКЕЫУЖЕЖДМЫКВДХВТЫЕДФЫЕРЗЛДЭМЫУДЗДПШЩНУДХВПЖЕЗЕДОЕВХЦЙФЗДПЫ ЫЩДГЖПЯЕДЭШЫЕЖЕЖЭЦДФЫ ЫЕЦ

### 13

АЧНГЧЕИХБЭТЛШЩИРЫПЭТЩТБЗИЧГБЭТАЧЕЧДЩЮТАЧТЩЕИЧГЩЩТКЧЕЛШГРУНР ЩЮТЩТАЧЫЩИЩХРТХБУРИЕПТШИЧТЭЩГТЕГБЗ ЩИРЫЖ ЧТГБЦЛЭР ТЧ ЩТНЛЭБМИТШИЧТЫМНЩТЕЗЧДЧН ЧТЗВДЩГБМИТЕЗЧЩСТАГРНЕИБЗЩИРЫРЮТЩЦТИРСТХТХЧЭЛТАЩИБМИТЧЕЧДЧРТНЧЗРГЩРТЧ ЩТАЧЫБКБМИТШИЧТЕБЭВРТЛЭ ВРТЕБЭВРТНРЫЖ ВРТЩЦТЙИЩСТЩЦДГБ ВСТЕИБ ЧЗПИЕПТЭЩ ЩЕИГБЭЩ

### 14

УИРГЯОЕШЭИРОЦРУИРЫЩЭЧОРЩЭМЕГЧЭЮРЙЖЗЩТУЕЭИЙЮУЦЫРЩЭРЯВИУЦЫРАУЧСРЬЩМИФЭМЯЖПЧЫРЩРГИЙЩМЩШРЧРЕГОЧУЧФЭ ЕЭЧМУЩШРНЧТУЧРЬЯФЭЮРВЧЭЕЖЭРИФЙЧРМЩФЬ ЧОЯЭРЧЫРАЕАРВЧФЭЦШРМЦОЦФИЙРМРЩГУЩОР ЛГЯРФР ЩОЕУЕОЧРЫЕССЕ ГЕРЧРЯДЙЙФЕРФЩВЧУИУЧЛОЧРЩРАЩФОЩФИРЧРЩРЬИПИ УЩОРВИЙЩМИАИРАУЧСЧРДЭЧРУЧАЩОЯРУИРЬЩМ ИГЛЭ

### 15

УНЮЧНДХЧБВШЛСНЙЛВЛВУМЮЛЭМЭЛВЦВНЮНС ЭЭНЮЙМВЙЛЧВШЛЮЙКЬМЦЛ ЙЮКВЦНВЦШ Ж ЭМВКЮЭНВЩЙНВНСХ ЖВ ВЭМЧЛЧВМДМВУНЩЙМВЭМЧЛЧВЭ ВЮЦКЕЛЭВЮВЩМЮДНЖВЦПУНДЭКРИМОВ ВДРЯ ТВЧНЬЯЛВЯ ДЛЙХВЭ Щ ЬНВЮНЦЮ ЖВЭ ВНСКЕЛЙ ДХЭНВД ЭМЙХЮКВЯ ДНВЙ ЖВЦЛАЭ ВМВЮДНАЭ ВЩ ЖВСНДХГ ВЦШ Ж ЭМВЭЛВЭ ЬНВНЙУБИ ЭН

### 16

ЧТПЖШЯНИВШЯДЧТЛЬШЯРВЮФТЯДЯ ЫЬЮЯЛГЫЭТВТЯЬТНШЖЯФТПОЖЯЗШЧЫЯЖТЖШЫЯЛХТЛЗГЫЯХЗШЯДЯ ЫЬЮЯЬЫЯНИВШЯЛЯЛШНШКЯУШЬЗОЖТЯЛД ЖОЯФШАЯ ШО ЯЛЗДВШ ЯЙЛЫЯЙПЫ ЮЯЖЗШЯЗШЯФОЬТВЯЙШУ ШЧЬШЯЮЯЛТ ТЯОЯЫЛВОЯНИЯ ЬЫЯФПОРВШЛГЯЫМЫЯОЯШЯУШЬЗОЖЫЯАД ТЗГЯЮЯНИЯЛШЙЛЫ ЯЛФЮЗОВТ

### 17

ОСНЭЖЗВЩЙХЖКЛВЭНВТНЧЬВХЖХВРНДЙ ЛЕВПЭЛСЬЭРЛХВХЖАСЗЗВЛВНРЭСЬТЮТЖЗЦШВЗВЭЮРЖСЖЦШВЙОТЖРЛРШЦЗВФЖВХЩЖЕВМЖЦЦЬЕДЖВТВПРНРВКНКЬДРВЗВЙЦСЮАЖСЖВЭСЬЦХВИРНВРНВЦВАЙКНКВЙЭЖСНВТВТНЧЙВЗВНУСЗДЙСЖЦШВЛВНЦРНСМЬДЬСЖВТЬСЛХНСЬЭДЮКВХЩНСЬКВХНВКДЬВЦРЩЬКЛРЬСШДНВЭСЮСВХЖХНЕВРНВРЛЭВТВМЬСНКВХНЦРБКЬ

### 18

ОЧЙЖЙЧМЦВГЦТГЧАВМИЖДЧЛЕЖЛЙОЭЛСЧКЮПЮИЧЦОФЧОЧЛВЙЯРЭЛСЧОМЧНЙВЕВ

ЧАВМИЖДРЧКПВМПРЗЦТГЧЕПРУИРЦОЦЧКПЮЛЙПРЦЦВЕВЧАОИРЧЦРЧФРЭЮЦЩЯВГ

ЧЕВЭВАЯЮЧУВЯЮГЛЯОГЧЯРПЙЖМОЯЧЯЭЮЙЗРЙТГЧЯЖПЕЖМТГЧАВМИЖБЦТГЧУЮЧ

КОИУРЗВЯЧЕПРУИРЦОЦЧПВЛЙВФЧАЧЛРУЮЦЩЧЦВЧАЧКЭЮЗРДЧЖМВЯЧДЖИЧЦЮОФ

ВАЮПЦВЧОЧЫОМОВЦВФОСЧКПВБЖЧМРФЮЙОЙЩЧЕЭЖФЭОАРС

### 19

ЗЩОМЧЙШЧЧЯЛФЕАИГЙМФМЧЩЙШСЩЮФИЗЩЫАЩЙФЗЩМБЩУЙЖЧЗНЩЫЙЯЭЗЙСЛЧАЕШЩБИАЙШЙМЛХОХЙЫФЬАПЙЯФЛЭЬЩЫГЙЧЫЙСЩЛШЭУЙСЩЛЩЖЙЫАДАЙЦШАЗБЦЙДЛФЮЫЭДЙАЙЛФЕЧЮФЛЧШФЫЫЭДЙСЩЛШЭУЙОЧШЧЛАЗЙАДЙЧЯЙХИЛФЮЩЫЫЭПЙЛФЖЧБИЦПЙАЙЧЯЙХШЦЖЬЩУЙБШЧЩУЙТЫЧБИАЙБШЩЛПЙИЧОЧЙЫЧБАЗЙЧЫЙЮЩЛЫЧЩЙМЧЗГ ЧЙБЙАЕЧЯЛФНЩЫАЩДЙДЩЛИШЧУЙОЧЗЧШЭ

### 20

ЙУЭОГ ВОРУГЖУГТБ ЦБЩЬГВГЙБРБЦЧЬГЭОЫЧГБШРУЩБТГЩУЙУРБ ЮГБСВЫУРВГ БРЖАУГЩУЩГАУЭЬЫТБЭАЧГБСВЫУДЦГКБ ПЫУЭОГО ЖБЬГЖЬШБГПЦЭЬЖЖООГ ТЬСЬ ЦЮГЭБ УГТЬЦЬЭБЩГВГХЬЖВЬГХЦВЯЬЩГЖУХБРЖОРВГ ЬЭЫАЬГРВЙЧГЛРУЫЬЖЯЬ ЩБФГТЬ ЬРБ ЦВДГШБО ЮГЩУЩБФГЖВШПЫЮГЙЖУЩБЛБФГТ ЦЭЬЯВГБЖУГЩУЙУРБ ЮГЖЬГИРУГУГРЬЦЬРУ

# Литература

[1] Stallings W, “Cryptography And Network Security. Principles And Practice”, 5th Edition, 2011.