

Министерство науки и высшего образования Российской Федерации
Ярославский государственный университет им. П. Г. Демидова
Кафедра алгебры и математической логики

С. И. Яблокова

**Задачи по криптографическим методам
защиты информации.
Симметричные криптосистемы**

Практикум

Ярославль
ЯрГУ
2020

УДК 004.056.5(076.5)
ББК 3973.2-018.2я73-4
Я14

Рекомендовано
Редакционно-издательским советом университета
в качестве учебного издания. План 2020 года

Рецензент
кафедра алгебры и математической логики
ЯрГУ Ярославского государственного университета им. П. Г. Демидова

Я14 **Яблокова, Светлана Ивановна.**

Задачи по криптографическим методам защиты информации. Симметрические крип-
тосистемы: практикум / С. И. Яблокова ; Яросл. гос. ун-т им. П. Г. Демидова. – Ярос-
лавль : ЯрГУ. – 2020. – 48 с.

Практикум содержит задачи по криптографическим методам защиты информации
и описание основных симметричных криптосистем, используемых при решении задач.
Приведены примеры с подробным разбором методов решения.

Предназначен для студентов, изучающих дисциплину «Криптографические методы
защиты информации».

УДК 004.056.5(076.5)
ББК 3973.2-018.2я73-4

Введение

В практикуме содержатся задачи по криптографическим методам защиты информации. Эта дисциплина изучается студентами специальности «Компьютерная безопасность» на четвертом курсе, студентами специальности «Информационная безопасность» на третьем курсе. Кроме того, она является одним из спецкурсов по выбору для студентов четвертого курса специальности «Математика и компьютерные науки».

Для решения предлагаемых в практикуме задач требуется знание основных исторических и современных криптосистем симметричного шифрования, знание определения и свойств сравнений по натуральному модулю, умение проводить вычисления в кольцах вычетов, умение использовать расширенный алгоритм Евклида, знание основных понятий алгебры. Задания, связанные с вычислениями в кольцах вычетов, как правило, вызывают наибольшие трудности.

Практикум начинается с напоминания основных криптосистем симметричного шифрования, которые даются в порядке их исторического появления. Каждая криптосистема иллюстрируется примерами использования алгоритма шифрования и алгоритма дешифрования. Большинство алгоритмов описано в терминах сравнений, что позволяет отказаться от большинства громоздких таблиц, которыми первоначально пользовались в этих криптосистемах. Далее предлагается набор заданий для самостоятельного решения, которые могут быть использованы для контрольных работ и экзаменационных заданий. В приложении приведены таблицы, которые можно использовать при шифровании и дешифровании в различных криптосистемах.

Исторические шифры замены

В поточных шифрах простой замены множества шифрвеличин и шифробозначений совпадают с алфавитом открытого текста \mathbb{A} . Ключом такого шифра является подстановка на множестве \mathbb{A} , верхняя строка которой представляет собой естественную последовательность букв алфавита, а нижняя – систематически перемешанную или случайную последовательность букв из \mathbb{A} .

Шифр Цезаря

Исторический шифр Цезаря заменял буквы открытого текста в соответствии с подстановкой, нижняя строка которой представляла собой алфавит открытого текста, сдвинутый циклически на 3 буквы влево. Для английского алфавита это подстановка:

$$\begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z & a & b & c \end{pmatrix},$$

для русского алфавита:

$$\begin{pmatrix} a & б & в & г & д & е & ё & ж & з & и & й & к & л & м & н & о & п & р & с & т & у & ф & х & ц & ч & ш & щ & ъ & ы & ь & э & ю & я \\ г & д & е & ё & ж & з & и & й & к & л & м & н & о & п & р & с & т & у & ф & х & ц & ч & ш & щ & ъ & ы & ь & э & ю & я & а & б & в \end{pmatrix}.$$

Буквы алфавита удобно отождествить с их числовыми эквивалентами (порядковыми номерами, начиная с 0) (см. табл. 1,2). Тогда шифрование по Цезарю можно записать просто формулой:

$$y_i \equiv x_i + 3 \pmod{n}, \quad (1)$$

где мощность алфавита \mathbb{A} , x_i – числовой эквивалент буквы открытого текста, y_i – числовой эквивалент соответствующей буквы шифртекста.

Для того, чтобы расшифровать криптограмму, полученную по формуле (1), очевидно, следует воспользоваться формулой:

$$y_i \equiv x_i - 3 \pmod{n}. \quad (2)$$

Пример 1. Используем исторический шифр Цезаря для шифрования фразы «*introduction to analysis*»

Поставим шифрвеличинам (буквам открытого текста) их числовые эквиваленты по таблице 2:

i n t r o d u c t i o n t o a n a l y s i s
8, 13, 19, 17, 14, 3, 20, 2, 19, 8, 14, 13 19, 14 0, 13, 0, 11, 24, 18, 8, 18

Теперь вычислим числовые эквиваленты шифробозначений по формуле (1), где $n = 26$ (количество букв в английском алфавите). В результате получим последовательность:

11, 16, 22, 20, 17, 6, 23, 5, 22, 11, 17, 16 22, 17 3, 16, 3, 14, 1, 21, 11, 21,

соответствующую (см. табл. 2) следующей криптограмме :

l q w u r g x f w l r q w r d q d o b v l v.

Пример 2. Расшифровать криптограмму

т з у л с ж л ь з ф н л м ы л ч у,

зашифрованную историческим шифром Цезаря.

Воспользуемся формулой (2) для вычисления числовых эквивалентов букв открытого текста. Буквам криптограммы соответствует числовая последовательность (см. табл. 1):

19, 8, 20, 12, 18, 7, 12, 27, 8, 21, 14, 12, 13 28, 12, 24, 20.

Количество букв в русском алфавите равно 33 , значит, $n = 33$. В результате вычислений получаем последовательность:

16, 5, 17, 9, 15, 4, 9, 24, 5, 18, 11, 9, 10 25, 9, 21, 17,

которая соответствует открытому тексту:

«периодический шифр».

Шифр Тритемия

Это многоалфавитный периодический шифр замены, правило зашифрования которого состоит в использовании периодически повторяющейся последовательности простых замен. Он основан на квадратной таблице, шифралфавиты которой записаны в строки таблицы один под другим, причём каждый из них циклически сдвинут на одну позицию влево по сравнению с предыдущим. Первая строка таблицы состоит из букв алфавита, записанных в естественном порядке (табл. 3,4). Первая буква открытого текста шифруется первым алфавитом, вторая буква – вторым, т.е. в первой строке находится буква открытого текста и заменяется стоящей под ней во второй строке буквой, и т.д. После использования последней строки таблицы, процесс вновь начинается с первой строки.

Процесс расшифрования выглядит следующим образом: первая буква открытого текста совпадает с первой буквой криптограммы, вторую букву криптограммы ищем во второй строке таблицы и находим стоящую над ней букву первой строки. Это будет вторая буква открытого текста. Третью букву криптограммы находим в третьей строке таблицы и берем в качестве соответствующей буквы открытого текста букву, стоящую над ней в первой строке, и т.д.

Пример 3. Зашифруем с помощью таблицы Тритемия (табл. 4) слово «*university*».

Первая буква ищется в первой строке таблицы и, очевидно, не меняется, т.е. это буква *u*. Вторую букву сообщения *n* ищем в первой строке, под ней во второй строке стоит буква *o*, это вторая буква криптограммы. Продолжая этот процесс, получим

u o k y i w u p b h.

Этот метод шифрования можно записать математической формулой:

$$y_i \equiv x_i + (i - 1) \pmod{n}, \quad (i = 1, 2, 3, \dots). \quad (3)$$

Действительно, вернёмся к примеру 3. Открытое сообщение можно записать соответствующей последовательностью числовых эквивалентов букв открытого текста:

20, 13, 8, 21, 4, 17, 18, 8, 19, 24.

Проведем вычисления по формуле (3):

$$\begin{aligned} y_1 &= 20 + 0 \equiv 20 \pmod{26}, & y_6 &= 17 + 5 \equiv 22 \pmod{26}, \\ y_2 &= 13 + 1 \equiv 14 \pmod{26}, & y_7 &= 18 + 6 \equiv 24 \pmod{26}, \\ y_3 &= 8 + 2 \equiv 10 \pmod{26}, & y_8 &= 8 + 7 \equiv 15 \pmod{26}, \\ y_4 &= 21 + 3 \equiv 24 \pmod{26}, & y_9 &= 19 + 8 \equiv 1 \pmod{26}, \\ y_5 &= 4 + 4 \equiv 8 \pmod{26}, & y_{10} &= 24 + 9 \equiv 7 \pmod{26}. \end{aligned}$$

В результате получим последовательность:

20, 14, 10, 24, 8, 22, 24, 15, 1, 7,

соответствующую криптограмме: *u o k y i w u p b h*.

Процесс расшифрования можно записать формулой:

$$x_i \equiv y_i - (i - 1)(\text{mod } n), \quad (i = 1, 2, 3, \dots). \quad (4)$$

Пример 4. Расшифровать криптограмму, зашифрованную по таблице Тритемия (табл.3):

n б т с н б.

Криптограмме соответствует числовая последовательность:

16, 1, 19, 18, 16, 1.

Пересчитаем ее по формуле (4), проводя вычисления по модулю $n = 33$ (мощность русского алфавита):

$$\begin{aligned} x_1 &= 16 - 1 \equiv 16 \pmod{33}, & x_4 &= 18 - 3 \equiv 15 \pmod{33}, \\ x_2 &= 1 - 1 \equiv 0 \pmod{33}, & x_5 &= 16 - 4 \equiv 12 \pmod{33}, \\ x_3 &= 19 - 2 \equiv 17 \pmod{33}, & x_6 &= 1 - 5 \equiv 29 \pmod{33}. \end{aligned}$$

В результате получаем последовательность:

16, 0, 17, 15, 12, 29,

соответствующую слову «пароль».

Шифр Белаза

Это многоалфавитный шифр с буквенным паролем (ключом). Паролем может служить слово или целая фраза. Пароль периодически записывается над открытым текстом. Буква пароля, расположенная над буквой текста, указывает на алфавит таблицы, который используется при шифровании этой буквы. Как правило, это алфавит из таблицы Тритемия, первой буквой которого является буква пароля. Обратная операция (расшифрование криптограммы) использует тот же пароль (ключ), который также периодически записывается над зашифрованным текстом. Буква пароля, стоящая над буквой криптограммы, указывает алфавит, которым она была зашифрована, т.е. строку таблицы Тритемия. В этой строке следует найти букву криптограммы, тогда стоящая в этом же столбце буква первой строки таблицы, даст соответствующую букву открытого текста.

Пример 5. Используя пароль (ключ) «*шест*», зашифровать по таблице Тритемия (табл.3) следующее сообщение: «*криптографическая защита*».

ш е с т ш е с т ш е с т ш е с т ш е с т ш е с
к р и п т о г р а ф и ч е с к а я з а щ и т а

Теперь воспользуемся таблицей 3. Первая буква пароля *ш*. В таблице ищем строку, начинающуюся с этой буквы. В верхней строке таблицы находим соответствующую букву открытого текста *к*; на пересечении столбца, в котором стоит буква *к* и строки, начинающиеся с буквы *ш*, находим букву *г*. Это и будет шифробозначение буквы *к*, т.е. первая буква криптограммы. Далее, берем строку, начинающуюся с буквы *е* и в первой строке находим букву *р*. На пересечении столбца с буквой *р* (в первой строке) и строки, начинающейся с *е*, находим следующую букву криптограммы *х* и т.д. В результате получим:

г х г в к у ф г б щ ъ й э ц ъ т ч м с л б ч с.

Пример 6. Расшифровать криптограмму, полученную на ключе “*task*” шифром Белазо:

v o f p b d w x m i s v b n x y k m s d b o f.

Запишем буквы пароля (ключа) над буквами криптограммы

t a s k t a s k t a s k t a s k t a s k t a s
v o f p b d w x m i s v b n x y k m s d b o f.

В таблице 4 ищем строку, начинающуюся с *t* и в ней первую букву криптограммы *v*. В первой строке таблицы в одном столбце с буквой *v* находится буква *c*. Это и есть первая буква открытого текста. Вторая буква пароля *a* является первой буквой алфавита, ей соответствует первая строка таблицы, значит, при шифровании вторая буква открытого текста не изменилась это буква *o*. Продолжая этот процесс, получим открытый текст

c o n f i d e n t i a l i n f o r m a t i o n.

Этот метод шифрования также можно описать математической формулой

$$y_i \equiv x_i + k_i \pmod{n} \quad (i=1,2,\dots), \quad (5)$$

где k_i – числовой эквивалент, соответствующий букве пароля, стоящей над i -й буквой открытого текста.

Соответственно, при расшифровании криптограммы следует использовать формулу

$$y_i \equiv x_i - k_i \pmod{n} \quad (i=1,2,\dots). \quad (6)$$

Проверим формулу (5) для последнего примера, т. е. зашифруем фразу «*confidential information*» на ключе “*task*”.

Открытому тексту соответствует числовая последовательность

2, 14, 13, 5, 8, 3, 4, 13, 19, 8, 0, 11 8, 13, 5, 14, 17, 12, 0, 19, 8, 14, 13,

а ключу числовая последовательность 19, 0, 18, 10.

Последовательно записывая числа ключа над соответствующими числами открытого текста, получаем таблицу

19	0	18	10	19	0	18	10	19	0	18	10		19	0	18	10	19	0	18	10	19	0	18
2	14	13	5	8	3	4	13	19	8	0	11		8	13	5	14	17	12	0	19	8	14	13

Складывая числа в каждом столбце по модулю 26 (мощность английского алфавита), получаем числовую последовательность

21, 14, 5, 15, 1, 3, 22, 23, 12, 8, 18, 21 1, 13, 23, 24, 10, 12, 18, 3, 1, 14, 5,

которая соответствует криптограмме :

v o f p b d w x m i s v b n x y k m s d b o f.

Шифр де ла Porta

Это шифр многоалфавитной замены, в котором используется прямоугольная таблица с периодически сдвигаемым смешанным алфавитом и паролем (ключом) (см. табл.5,6).

Шифрование осуществляется с помощью ключа, буквы которого периодически записываются над буквами открытого текста. Буква ключа определяет алфавит (заглавная буква первого столбца таблиц 5,6), расположенная под ней буква открытого текста ищется в верхнем или нижнем полуалфавите и заменяется соответствующей (стоящей в том же столбце) буквой второго полуалфавита.

В исторической таблице де ла Porta (табл.5) алфавит состоял из 24 букв, в ней отсутствовали буквы *j* и *v*, которые при шифровании заменялись соответственно буквами *i* и *w*. Кроме того, буква *w* стояла в конце алфавита. Если добавить в таблицу буквы *j* и *v* и не менять алфавитного порядка букв английского языка, то получим таблицу 6.

Процесс расшифрования криптограммы аналогичен процессу шифрования.

Пример 7. Шифром де ла Porta, используя таблицу 5, зашифровать на ключе “*vigener*” сообщение «*information*».

Запишем буквы ключа над буквами сообщения:

$$\begin{array}{c} v i g e n e r v i g e \\ i n f o r m a t i o n . \end{array}$$

В таблице 5 находим в левом столбце строку, содержащую букву *w* (замена буквы *v*) и в найденной двойной строке ищем букву *i*. Она находится в верхнем полуалфавите, под ней стоит буква *u*. Она и будет первой буквой криптограммы. Далее, ищем букву *i* в левом столбце и в соответствующей двойной строке находим букву *n* она стоит в нижнем полуалфавите, над ней находится буква *i* это будет вторая буква криптограммы. Продолжая, получим

$$u i x m l o x h n l l .$$

Если для шифрования воспользоваться таблицей 6, то получим другую криптограмму

$$s j v m l o v j z l l .$$

Шифр Виженера

Это многоалфавитный шифр замены с буквенным паролем (ключом). Простейший вариант основан на квадратной таблице, подобной таблице Тритемия, к которой для удобства добавлена вверху строка с алфавитом открытого текста, а слева добавлен столбец с алфавитом ключа (табл. 7, 8). Такую таблицу называют таблицей Виженера. Шифрование проводится так же, как в случае шифра Белазо.

Другой вариант шифра Виженера – это шифрование *самоключом*. В этом случае в качестве ключа выступает само открытое сообщение с добавленной к нему в качестве первой буквы одной из букв алфавита, известной отправителю и получателю. Если сообщение имеет вид

$$M = m_1 m_2 m_3 \dots m_i \dots ,$$

а ключ (первая буква) есть m_0 , то последовательности букв $K = m_0 m_1 m_2 m_3 \dots m_i \dots$ и M подписываются друг под другом

$$\begin{array}{c|c} K & m_0 m_1 m_2 m_3 \dots m_i \dots \\ M & m_1 m_2 m_3 m_4 \dots m_i \dots \end{array}$$

Пара букв, стоящих друг под другом в K и M указывают, соответственно, строку и столбец таблицы Виженера, на пересечении которых находится знак шифрованного текста.

Пример 8. Самоключом Виженера зашифровать сообщение *today*, взяв в качестве ключа букву *k*.

Запишем последовательности ключа и сообщения друг под другом

$$\begin{array}{c|c} K & k t o d a \\ M & t o d a y \end{array}$$

По таблице Виженера (табл.8) на пересечении строки *k* со столбцом *t* находим букву *d*; на пересечении строки *t* со столбцом *o* находим букву *h*; на пересечении строки *o* и столбца *d* находим букву *r* и т.д. В результате получаем криптограмму

$$d h r d y .$$

Здесь также можно обойтись без таблицы Виженера, используя таблицу 2. Сопоставим всем буквам ключа и сообщения их числовые эквиваленты по таблице 2, получим пару строк

$$\begin{array}{c|c} K & 10 19 14 3 0 \\ M & 19 14 3 0 24 \end{array}$$

Складывая в каждом столбце числа по модулю 26, получаем последовательность чисел 3, 7, 17 3, 24, соответствующую криптограмме .

$$d h r d y$$

Обобщенный шифр Цезаря

Шифр Цезаря (или сдвиговой шифр) можно обобщить, если выбирать длину сдвига (ключа) произвольно. Пусть ключ $\alpha \in \mathbb{Z}_n$, тогда формула шифрования принимает вид

$$y_i \equiv x_i + \alpha \pmod{n}, \quad (7)$$

где x_i – числовой эквивалент буквы открытого текста, y_i – числовой эквивалент соответствующей буквы шифртекста, n – мощность алфавита.

Обратная операция (расшифрование) задается формулой

$$x_i \equiv y_i - \alpha \pmod{n}. \quad (8)$$

Пример 9. На ключе $\alpha = 7$ обобщенным шифром Цезаря зашифровать сообщение *cryptography*.

Сообщению соответствует числовая последовательность

2, 17, 24, 15, 19, 14, 6, 17, 0, 15, 7, 24.

Применим формулу (7) с $\alpha = 7$, тогда получим последовательность

9, 24, 5, 22, 0, 21, 13, 24, 7, 22, 14, 5,

соответствующую криптограмме *j y f w a v n y h w o f*.

Аффинный поточный шифр

Ключом этого шифра является пара элементов $\alpha, \beta \in \mathbb{Z}_n$, причем α должно быть обратимо по модулю n , т.е. $\alpha \in \mathbb{Z}_n^*$.

Формула шифрования принимает вид

$$y_i \equiv \alpha x_i + \beta \pmod{n}. \quad (9)$$

Обратная операция задается формулой

$$x_i \equiv \alpha^{-1} (y_i - \beta) \pmod{n}. \quad (10)$$

Пример 10. На ключе $\alpha = 3$, $\beta = 5$ зашифровать аффинным поточным шифром слово *cryptography*.

Как мы видели в примере 9, этому слову соответствует числовая последовательность

2, 17, 24, 15, 19, 14, 6, 17, 0, 15, 7, 24.

Применим формулу (9) к каждому числу нашей последовательности:

$$\begin{aligned} 3 \cdot 2 + 5 &\equiv 11 \pmod{26}, & 3 \cdot 17 + 5 &\equiv 4 \pmod{26} \\ 3 \cdot 24 + 5 &\equiv 25 \pmod{26}, & 3 \cdot 15 + 5 &\equiv 24 \pmod{26}, \\ 3 \cdot 19 + 5 &\equiv 10 \pmod{26}, & 3 \cdot 14 + 5 &\equiv 21 \pmod{26}, \\ 3 \cdot 6 + 5 &\equiv 23 \pmod{26}, & 3 \cdot 0 + 5 &\equiv 5 \pmod{26}, \\ 3 \cdot 7 + 5 &\equiv 0 \pmod{26}. \end{aligned}$$

В результате получаем последовательность

11, 4, 25, 24, 10, 21, 23, 4, 5, 24, 0, 25,

соответствующую криптограмме *l e z y k v x e f y a z*.

Пример 11. Расшифровать криптограмму *з ё н ё ч д я ь щ ь с й*, полученную на ключе $\alpha = 2$, $\beta = 9$ с помощью аффинного поточного шифра ($n = 33$).

Сначала найдем элемент, обратный к α по модулю 33. Очевидно,

$$2^{-1} \equiv 17 \pmod{33}.$$

Теперь формула (10) принимает вид

$$x_i \equiv 17(y_i - 9) \pmod{33}.$$

Криптограмме соответствует числовая последовательность (см. табл. 1)

8, 6, 14, 6, 24, 4, 32, 29 26, 27, 18, 10.

Тогда

$$\begin{array}{ll} x_1 \equiv 17(8-9) \equiv 16 \pmod{33}, & x_2 \equiv 17(6-9) \equiv 15 \pmod{33}, \\ x_3 \equiv 17(14-9) \equiv 19 \pmod{33}, & x_4 \equiv 17(6-9) \equiv 15 \pmod{33}, \\ x_5 \equiv 17(24-9) \equiv 24 \pmod{33}, & x_6 \equiv 17(4-9) \equiv 14 \pmod{33}, \\ x_7 \equiv 17(32-9) \equiv 28 \pmod{33}, & x_8 \equiv 17(29-9) \equiv 10 \pmod{33}, \\ x_9 \equiv 17(26-9) \equiv 25 \pmod{33}, & x_{10} \equiv 17(27-9) \equiv 9 \pmod{33}, \\ x_{11} \equiv 17(18-9) \equiv 21 \pmod{33}, & x_{12} \equiv 17(10-9) \equiv 17 \pmod{33}. \end{array}$$

Получаем числовую последовательность

16, 15, 19, 15, 24, 14, 28, 10, 25, 9, 21, 17,

соответствующую тексту *поточный шифр*.

Блочные шифры простой замены

Шифр Плейфера

Это простейший блочный шифр, оперирующий с биграммными шифробозначениями. Основой этого шифра является прямоугольная таблица, в которую записан систематически перемешанный алфавит.

Систематическое перемешивание означает следующее: берётся некоторое ключевое слово, не содержащее одинаковых букв, либо, если в нём есть одинаковые буквы, то при повторном появлении они отбрасываются. Это слово записывается в таблицу, за ним записываются не вошедшие в ключевое слово буквы алфавита в естественном (алфавитном) порядке.

При шифровании открытый текст представляется в виде последовательности биграмм (двух рядом стоящих букв). Если текст имеет нечётную длину или содержит бигramму, состоящую из одинаковых букв, то в него добавляются “пустышки”. Пустышкой является некоторая редкая для данного текста (или языка) буква. Пустышка вставляется между одинаковыми буквами биграммы или добавляется в текст для того, чтобы его длина стала чётной.

Правило шифрования

Буквы биграммы (i, j) ($i \neq j$), являющиеся шифрвеличиной, находятся в таблице. Биграмма (i, j) заменяется при шифровании биграммой (k, l) , где k и l определяются следующим образом:

1. Если i и j не лежат в одной строке или столбце таблицы, то их позиции образуют противоположные вершины прямоугольника. Тогда k и l – другая пара вершин этого прямоугольника, где k – вершина, лежащая в одной строке с i

$$\begin{array}{l} i \rightarrow k \\ l \leftarrow j \end{array}$$

2. Если i и j лежат в одной строке, то k и l – буквы той же строки, расположенные непосредственно справа от i и j соответственно. Если одна из букв – последняя в строке, то её правым соседом является первая буква той же строки.

3. Если i и j лежат в одном столбце, то они заменяются соседними буквами снизу. Если одна из букв i или j – последняя буква столбца, то её соседом снизу является первая буква того же столбца.

Алгоритм расшифрования

В случае (1) биграмма (k, l) заменяется на бигramму (i, j) , где i и j – вершины прямоугольника, двумя противоположными вершинами которого являются k и l , причём i лежит в одной

строке с k . Во втором случае k и l следует заменить соседними буквами слева, если одна из них является первой буквой строки, то её соседом слева является последняя буква той же строки. В третьем случае k и l следует заменить соседними буквами сверху, если одна из них – первая буква столбца, то её соседом сверху является последняя буква того же столбца.

Пример 12. Рассмотрим русский алфавит, выбросив из него 3 буквы: ё, й, ъ. Оставшиеся 30 букв запишем в таблицу 5×6 , систематически перемешав алфавит на основе ключевого слова «икосаэдр»:

И	К	О	С	А	Э
Д	Р	Б	В	Г	Е
Ж	З	Л	М	Н	П
Т	У	Ф	Х	Ц	Ч
Ш	Щ	Ы	Ь	Ю	Я

Зашифруем фразу «блочный шифр». Здесь 11 букв, поэтому следует дополнить его до чётной длины, т. е. вставить пустышку. В качестве пустышки возьмём, например, букву ϕ , которая достаточно редко встречается, и сразу разобьём текст на биграммы:

бл оч ны йф ши фр.

Поскольку в таблице отсутствует буква $й$, то заменим её при шифровании буквой $и$. Буквы первой биграммы стоят в одном столбце. Согласно правилу, заменяем их буквами $л$ и ϕ соответственно. Буквы второй биграммы образуют вершины прямоугольника, другие две его вершины $э$ и ϕ , причём $э$ лежит в одной строке с $о$. Буквы третьей, четвёртой и шестой биграмм также заменяются по правилу прямоугольника. Буквы пятой биграммы стоят в одном столбце таблицы. Мы должны заменить их соседними буквами снизу, но $ш$ – последняя буква столбца, значит, она заменяется первой буквой того же столбца $и$.

В результате получаем криптограмму

л ф э ф л ю о т и д у б

Пример 13. Расшифруем полученную на том же ключе криптограмму

а ж ы б в з г ю э и.

Разобьём текст на биграммы: *а ж ыб в з гю эи.*

Буквы $а$ и $ж$ образуют противоположные вершины прямоугольника, значит, их следует заменить на $и$ и $н$ соответственно. Буквы $ы$ и $б$ стоят в одном столбце, они заменяются соседями сверху, т.е. на ϕ и $о$ соответственно. По правилу прямоугольника биграмма *вз* переходит в биграмму *рм*. Буквы $г$ и $ю$ следующей биграммы стоят в одном столбце таблицы, значит, соответственно заменяются на $а$ и $ц$. Последняя биграмма преобразуется по правилу прямоугольника, т.е. *эи* переходит в *ия*. Итак, получаем открытое сообщение:

информация.

Шифр Хилла

Шифрвеличинами этого шифра являются k -граммы открытого текста ($k \geq 2$), буквы которых представлены числовыми эквивалентами. (Буквы алфавита открытого текста сопоставляются элементам кольца вычетов \mathbb{Z}_n , где n – мощность алфавита.)

Правило шифрования – это линейное преобразование кольца \mathbb{Z}_n . Если $x = (x_1, x_2, \dots, x_k)$ – k -грамма открытого текста, $y = (y_1, y_2, \dots, y_k)$ – k -грамма шифртекста, а $A = (a_{ij})$ – обратимая в \mathbb{Z}_n квадратная матрица порядка k , то

$$y^T = A x^T. \quad (11)$$

Очевидно, ключом этого шифра является матрица A .

Расшифровать k -грамму можно с помощью обратного преобразования

$$x^T = A^{-1} y^T. \quad (12)$$

Здесь A^{-1} – матрица, обратная к A в \mathbb{Z}_n . Все операции проводятся в кольце \mathbb{Z}_n .

Пример 14. Пусть $k = 3$. В качестве ключа шифра Хилла возьмем матрицу

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 1 \\ 3 & 7 & 5 \end{pmatrix}.$$

Зашифруем фразу

the different meaning.

Разобьем открытый текст на 3-граммы:

the dif fer ent mea nin g.

В последней группе всего одна буква, следует дополнить ее до 3-граммы пустышками. В качестве пустышек возьмем буквы *zz*. Заменяя буквы 3-грамм их числовыми эквивалентами из кольца \mathbb{Z}_{26} , получаем последовательности

19, 7, 4 3, 8, 5 5, 4, 17 4, 13, 19 12, 4, 0 13, 8, 13 6, 25, 25.

Открытый текст запишем по столбцам в матрицу X :

$$X = \begin{pmatrix} 19 & 3 & 5 & 4 & 12 & 13 & 6 \\ 7 & 8 & 4 & 13 & 4 & 8 & 25 \\ 4 & 5 & 17 & 19 & 0 & 13 & 25 \end{pmatrix}.$$

Теперь по формуле (11) получим 3-граммы шифртекста в столбцах матрицы $Y = AX$, проводя вычисления в кольце \mathbb{Z}_{26} :

$$Y = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 1 \\ 3 & 7 & 5 \end{pmatrix} \begin{pmatrix} 19 & 3 & 5 & 4 & 12 & 13 & 6 \\ 7 & 8 & 4 & 13 & 4 & 8 & 25 \\ 4 & 5 & 17 & 19 & 0 & 13 & 25 \end{pmatrix} = \begin{pmatrix} 19 & 8 & 12 & 9 & 20 & 16 & 1 \\ 25 & 25 & 21 & 14 & 18 & 1 & 6 \\ 22 & 12 & 24 & 16 & 12 & 4 & 6 \end{pmatrix}.$$

Теперь можно записать полученные столбцы в строку, заменяя числа соответствующими буквами английского алфавита:

t z w i z m m v y j o q u s m q b e b g g.

Пример 15. Расшифровать криптограмму

y x w f t f w d n,

полученную шифром Хилла на ключе $A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 4 & 8 & 5 \end{pmatrix}$.

Поскольку порядок матрицы равен 3, то шифровались 3-граммы открытого текста. Используется английский алфавит, значит, вычисления производятся в кольце \mathbb{Z}_{26} . Чтобы прочитать криптограмму, воспользуемся формулой (12).

Обратная к матрице A в \mathbb{Z}_{26} есть

$$A^{-1} = \begin{pmatrix} 9 & -1 & 9 \\ -1 & -2 & 1 \\ 10 & 4 & 7 \end{pmatrix}.$$

Разделим текст криптограммы на 3-граммы

yxw ftf wdn,

заменим буквы их числовыми эквивалентами из \mathbb{Z}_{26} и поместим 3-граммы в столбцы матрицы Y :

$$Y = \begin{pmatrix} 24 & 5 & 22 \\ 23 & 19 & 3 \\ 22 & 5 & 13 \end{pmatrix}.$$

Тогда

$$X = A^{-1}Y = \begin{pmatrix} 9 & -1 & 9 \\ -1 & -2 & 1 \\ 10 & 4 & 7 \end{pmatrix} \begin{pmatrix} 24 & 5 & 22 \\ 23 & 19 & 3 \\ 22 & 5 & 13 \end{pmatrix} = \begin{pmatrix} 1 & 19 & 0 \\ 4 & 14 & 11 \\ 18 & 5 & 11 \end{pmatrix}$$

и, выписывая полученные 3-граммы в строку, получаем

$$1, 4, 18, 19, 14, 5, 0, 11, 11$$

или *best of all*.

Криптограмму, полученную шифром Хилла, можно перешифровать еще раз, используя другой ключ, т.е. получить двойное шифрование. Для двойного шифрования нам нужно два ключа. Пусть A и B квадратные матрицы порядка k . Шифрование k -грамм открытого текста проводится по формуле

$$y^T = BAx^T. \quad (13)$$

Тогда обратная операция (расшифрование) задается формулой

$$x^T = A^{-1}(B^{-1}y^T) = (A^{-1}B^{-1})y^T. \quad (14)$$

Пример 16. Расшифровать криптограмму

н ч м н ц щ р ч,

полученную двойным шифром Хилла на ключах

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix} \quad \text{и} \quad B = \begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix}.$$

Используется русский алфавит, значит $n = 33$. Порядок матриц равен 2, т.е. шифровались биграммы. Найдем A^{-1} и B^{-1} в кольце \mathbb{Z}_{33} .

Очевидно,

$$A^{-1} = \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 2 & -1 \\ -7 & 4 \end{pmatrix}.$$

Тогда

$$A^{-1}B^{-1} = \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -7 & 4 \end{pmatrix} = \begin{pmatrix} -24 & 13 \\ 13 & -7 \end{pmatrix} = \begin{pmatrix} 9 & 13 \\ 13 & -7 \end{pmatrix}$$

в \mathbb{Z}_{33} . Разобьем криптограмму на биграммы и заменим буквы их числовыми эквивалентами из кольца \mathbb{Z}_{33} :

$$\begin{array}{cc} \text{н ч} & \text{м н} & \text{ц щ} & \text{р ч} \\ 14, 24 & 13, 14 & 23, 26 & 17, 27 \end{array}$$

Тогда

$$X = \begin{pmatrix} 9 & 13 \\ 13 & -7 \end{pmatrix} \begin{pmatrix} 14 & 13 & 23 & 17 \\ 24 & 14 & 26 & 27 \end{pmatrix} = \begin{pmatrix} 9 & 2 & 17 & 9 \\ 14 & 5 & 18 & 32 \end{pmatrix}$$

в \mathbb{Z}_{33} , что соответствует тексту *и н в е р с и я*.

Аффинный блочный шифр

Этот шифр является обобщением шифра Хилла, т. е. это тоже блочный шифр, шифрующий m -граммы открытого текста по правилу

$$y^T \equiv Ax^T + b^T \pmod{n}, \quad (15)$$

где $x = (x_1, x_2, \dots, x_m)$ m -грамма открытого текста, $y = (y_1, y_2, \dots, y_m)$ m -грамма зашифрованного текста, A – квадратная матрица порядка m и $b = (b_1, b_2, \dots, b_m)$ – вектор длины m . Ключом этого шифра является пара A, b . Обратная операция (расшифрование криптограммы) применяется к m -граммам криптограммы по правилу

$$x^T \equiv A^{-1}(y^T - b^T) \pmod{n}. \quad (16)$$

Здесь A^{-1} – матрица обратная к A в кольце \mathbb{Z}_n .

Пример 17. Расшифровать криптограмму

lvosp x h u v j n t c n n b v v,

полученную аффинным блочным шифром на ключе

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 5 & 2 \\ 3 & 3 & 2 \end{pmatrix}, \quad b^T = \begin{pmatrix} 5 \\ 11 \\ 8 \end{pmatrix}.$$

Нам потребуется матрица A , обратная к A в кольце \mathbb{Z}_{26} . Нетрудно проверить, что это матрица

$$A^{-1} = \begin{pmatrix} -4 & 1 & 1 \\ -2 & 1 & 0 \\ 9 & -3 & -1 \end{pmatrix}.$$

Разобьем криптограмму на 3-граммы

lv o s p x h u v j n t c n n b v v

и в столбцы матрицы поставим числовые эквиваленты букв каждой 3-граммы (из кольца \mathbb{Z}_{26})

$$Y = \begin{pmatrix} 11 & 18 & 7 & 9 & 2 & 1 \\ 21 & 15 & 20 & 13 & 13 & 21 \\ 14 & 23 & 21 & 12 & 13 & 21 \end{pmatrix}.$$

Теперь из каждого столбца матрицы Y вычтем вектор b^T :

$$\begin{pmatrix} 6 & 13 & 2 & 4 & 23 & 22 \\ 10 & 4 & 9 & 2 & 2 & 10 \\ 6 & 15 & 13 & 4 & 5 & 13 \end{pmatrix}.$$

К полученной матрице применим A^{-1} :

$$\begin{aligned} X &= \begin{pmatrix} -4 & 1 & 1 \\ -2 & 1 & 0 \\ 9 & -3 & -1 \end{pmatrix} \begin{pmatrix} 6 & 13 & 2 & 4 & 23 & 22 \\ 10 & 4 & 9 & 2 & 2 & 10 \\ 6 & 15 & 13 & 4 & 5 & 13 \end{pmatrix} = \\ &= \begin{pmatrix} -8 & 19 & 14 & -10 & 19 & 13 \\ -2 & 4 & 5 & -6 & 8 & 18 \\ 18 & -14 & -22 & 0 & 14 & -1 \end{pmatrix} = \begin{pmatrix} 18 & 19 & 14 & 16 & 19 & 13 \\ 24 & 4 & 5 & 20 & 8 & 18 \\ 18 & 12 & 4 & 0 & 14 & 25 \end{pmatrix}. \end{aligned}$$

В результате, заменяя числа столбцов на соответствующие буквы и записывая 3-граммы последовательно в строку, получаем

system of equations(z).

Очевидно, последняя буква является пустышкой, которая была добавлена в открытый текст.

Свойство линейности шифров Хилла и аффинного блочного шифров позволяет провести довольно эффективную атаку на эти шифры, т.е. попробовать найти ключ.

Криптоатака

Пусть нам известно, что шифруются m -граммы открытого текста и, кроме того, известны по крайней мере $m+1$ m -грамм открытого текста и соответствующие им m -граммы шифрованного текста. Пусть $x_{(0)}, x_{(1)}, \dots, x_{(m)}$ m -граммы открытого текста, $y_{(0)}, y_{(1)}, \dots, y_{(m)}$ – соответствующие m -граммы шифрованного текста, A и b – неизвестный ключ. Так как

$$y_{(i)}^T = Ax_{(i)}^T + b^T \quad (i = 0, 1, \dots, m),$$

то

$$y_{(i)}^T - y_{(0)}^T = (Ax_{(i)}^T + b^T) - (Ax_{(0)}^T + b^T) = A(x_{(i)}^T - x_{(0)}^T) \quad (i = 1, 2, \dots, m). \quad (17)$$

Введем обозначения:

$$\begin{aligned} y^{(i)} &= y_{(i)}^T - y_{(0)}^T & (i = 1, \dots, m), \\ x^{(i)} &= x_{(i)}^T - x_{(0)}^T & (i = 1, \dots, m). \end{aligned}$$

В новых обозначениях формула (17) переписывается в виде

$$y^{(i)} = Ax^{(i)} \quad (i = 1, \dots, m). \quad (18)$$

Запишем векторы $y^{(i)}$ ($i = 1, \dots, m$) в столбцы матрицы Y

$$Y = (y^{(1)} y^{(2)} \dots y^{(m)}),$$

а векторы $x^{(i)}$ ($i = 1, \dots, m$) – в столбцы матрицы X

$$X = (x^{(1)} x^{(2)} \dots x^{(m)}),$$

тогда соотношения (18) запишутся в виде матричного уравнения

$$Y = AX, \quad (19)$$

где неизвестной является матрица A

X – это квадратная матрица порядка m , если она обратима в кольце \mathbb{Z}_n , то можно найти A . Действительно, из (19) имеем

$$YX^{-1} = A.$$

Осталось найти вектор b . Для этого воспользуемся равенством

$$y_{(0)}^T = Ax_{(0)}^T + b^T,$$

откуда

$$b^T = y_{(0)}^T - Ax_{(0)}^T.$$

Пример 18. Известно, что при шифровании триграммы

act, cdu, bcu, adv

переходят соответственно в триграммы *avi, eua, cxx, dxa*.

Найти ключ аффинного блочного шифра и прочитать сообщение, зашифрованное на этом ключе

urwhwr yd isl xckyjgt qi mczjqon.

Поскольку даны 3-граммы открытого текста, которые переходят в 3-граммы шифртекста, то матрица должна быть порядка 3. Очевидно, что используется английский алфавит, т.е. $n = 26$.

Выпишем векторы $x_{(0)}, \dots, x_{(3)}$ и $y_{(0)}, \dots, y_{(3)}$:

$$\begin{aligned} x_{(0)} &= (0, 2, 19), x_{(1)} = (2, 3, 20), x_{(2)} = (1, 2, 20), x_{(3)} = (0, 3, 21), \\ y_{(0)} &= (0, 21, 20), y_{(1)} = (4, 24, 0), y_{(2)} = (2, 23, 23), y_{(3)} = (3, 23, 0). \end{aligned}$$

Найдем $x^{(i)}, y^{(i)}$ ($i = 1, 2, 3$):

$$x^{(1)} = x_{(1)}^T - x_{(0)}^T = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, x^{(2)} = x_{(2)}^T - x_{(0)}^T = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, x^{(3)} = x_{(3)}^T - x_{(0)}^T = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix},$$

$$y^{(1)} = y_{(1)}^T - y_{(0)}^T = \begin{pmatrix} 4 \\ 3 \\ 6 \end{pmatrix}, y^{(2)} = y_{(2)}^T - y_{(0)}^T = \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix}, y^{(3)} = y_{(3)}^T - y_{(0)}^T = \begin{pmatrix} 3 \\ 2 \\ 6 \end{pmatrix}.$$

Теперь матричное уравнение (19) имеет вид

$$\begin{pmatrix} 4 & 2 & 3 \\ 3 & 2 & 2 \\ 6 & 3 & 6 \end{pmatrix} = A \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

Нетрудно проверить, что в \mathbb{Z}_{26}

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 9 & -8 & -9 \\ 9 & -10 & -8 \\ -9 & 9 & 9 \end{pmatrix}, \text{ тогда}$$

$$A = \begin{pmatrix} 4 & 2 & 3 \\ 3 & 2 & 2 \\ 6 & 3 & 6 \end{pmatrix} \begin{pmatrix} 9 & -8 & -9 \\ 9 & -10 & -8 \\ -9 & 9 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 2 & 2 \end{pmatrix}.$$

Найдем вектор b :

$$b^T = y_{(0)}^T - Ax_{(0)}^T = \begin{pmatrix} 0 \\ 21 \\ 20 \end{pmatrix} - \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 2 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 0 \\ 21 \\ 20 \end{pmatrix} - \begin{pmatrix} 21 \\ 19 \\ 16 \end{pmatrix} = \begin{pmatrix} 5 \\ 2 \\ 4 \end{pmatrix}.$$

Значит, мы нашли ключ аффинного блочного шифра. Для того чтобы прочитать (расшифровать) криптограмму, нам потребуется матрица, обратная к A . Находим

$$A^{-1} = \begin{pmatrix} 2 & 0 & -1 \\ 1 & -1 & 0 \\ -2 & 1 & 1 \end{pmatrix}.$$

Разобьем криптограмму на 3-граммы

arw hwr ydi slx cky jgt qim czj qon,

заменяем каждую 3-грамму последовательностью числовых эквивалентов, входящих в неё букв, и поставим эти тройки в столбцы матрицы

$$\begin{pmatrix} 20 & 7 & 24 & 18 & 2 & 9 & 16 & 2 & 16 \\ 17 & 22 & 3 & 11 & 10 & 6 & 8 & 25 & 14 \\ 22 & 17 & 8 & 23 & 24 & 19 & 12 & 9 & 13 \end{pmatrix}.$$

Из каждого столбца полученной матрицы вычтем вектор b^T :

$$\begin{pmatrix} 15 & 2 & 19 & 13 & 23 & 4 & 11 & 23 & 11 \\ 15 & 20 & 1 & 9 & 8 & 4 & 6 & 23 & 12 \\ 18 & 13 & 4 & 19 & 20 & 15 & 8 & 5 & 9 \end{pmatrix}.$$

К последней матрице слева применяем матрицу A^{-1} :

$$\begin{pmatrix} 2 & 0 & -1 \\ 1 & -1 & 0 \\ -2 & 1 & 1 \end{pmatrix} \begin{pmatrix} 15 & 2 & 19 & 13 & 23 & 4 & 11 & 23 & 11 \\ 15 & 20 & 1 & 9 & 8 & 4 & 6 & 23 & 12 \\ 18 & 13 & 4 & 19 & 20 & 15 & 8 & 5 & 9 \end{pmatrix}$$

$$= \begin{pmatrix} 12 & 17 & 8 & 7 & 0 & 19 & 14 & 15 & 13 \\ 0 & 8 & 18 & 4 & 15 & 0 & 5 & 0 & 25 \\ 3 & 3 & 19 & 2 & 8 & 11 & 18 & 8 & 25 \end{pmatrix}.$$

Заменяя числовые эквиваленты буквами и записывая полученные 3-граммы последовательно в строку, получаем

Madrid is the capital of Spain(zz).

Задачи для самостоятельного решения

Задание 1

Зашифровать сообщение шифром Цезаря:

- | | |
|--|--------------------------------|
| 1. <i>separation axioms</i> ; | 11. десятичная дробь; |
| 2. <i>factor space</i> ; | 12. действительное число; |
| 3. <i>homeomorphic image</i> ; | 13. мощность множества; |
| 4. <i>classification of homeomorphisms</i> ; | 14. предел последовательности; |
| 5. <i>isotopy class</i> ; | 15. степенная функция; |
| 6. <i>polygonal knot</i> ; | 16. рациональная дробь; |
| 7. <i>composition of two knots</i> ; | 17. комплексное число; |
| 8. <i>two – dimensional surface</i> ; | 18. счетное множество; |
| 9. <i>basic concepts</i> ; | 19. упорядоченное множество; |
| 10. <i>rational function</i> ; | 20. непрерывная дробь. |

Задание 2

Расшифровать сообщение, зашифрованное шифром Цезаря:

1. ж л ч ч з у з р и ц л г о ч и р н и ц л л ;
2. х с т с о с ё л ь з ф н с з т у с ф х у г р ф х е с ;
3. т у с л к е с ж р г в ч и р н и ц л л ;
4. р с у п л у с е г р р с з т у с ф х у г р ф х е с ;
5. е ю т ц н о с з н р с й з ф х е с ;
6. п г н ф л н ц н ч и р н и ц л л ;
7. н с п т г н х р с з н р с й з ф х е с ;
8. ф з т г у г д з о я р с ф х я ;
9. п з х с ж л х з у г и ц л л ;
10. п з х у л ь з ф н с з т у с ф х у г р ф х е с ;
11. l q w u r g x f w l r q w r w r s r o r j b ;
12. f r q f h s w r i v s d f h ;
13. w r s r o r j l f d o v s d f h ;
14. u l h p d q q v x u i d f h ;
15. j h q h u d o w r s r o r j b ;
16. f o d v v l i l f d w l r q r i v x u i d f h v ;
17. r u e l w v s d f h v ;
18. s u r m h f w l y h v s d f h ;
19. p h w u l f v s d f h ;
20. f r q w l q x r x v p d s s l g j v .

Задание 3

Зашифровать сообщение шифром Тритемия:

- | | |
|------------------------------|------------------------------|
| 1. <i>compartification</i> ; | 11. унитарное пространство; |
| 2. <i>property</i> ; | 12. билинейная форма; |
| 3. <i>algebra</i> ; | 13. сопряжённое число; |
| 4. <i>commutator</i> ; | 14. фундаментальное решение; |

- | | |
|-----------------------------|--------------------------------------|
| 5. <i>polyhedron</i> ; | 15. <i>аффинные координаты</i> ; |
| 6. <i>cylinder</i> ; | 16. <i>каноническое уравнение</i> ; |
| 7. <i>partition</i> ; | 17. <i>индуцированный оператор</i> ; |
| 8. <i>covering</i> ; | 18. <i>разложение определителя</i> ; |
| 9. <i>preliminary</i> ; | 19. <i>симметрическая матрица</i> ; |
| 10. <i>characteristic</i> ; | 20. <i>определитель Грама</i> . |

Задание 4

Расшифровать сообщение, зашифрованное шифром Тритемия:

- | | |
|--|--|
| 1. <i>и т у о и и ф и з ц т н</i> ; | 11. <i>g f p h v f r p h j d t a</i> ; |
| 2. <i>ф б м х т х о о з я т й</i> ; | 12. <i>c p o s p j z l v n c d</i> ; |
| 3. <i>д н м г л е ш л у е ы э н ы</i> ; | 13. <i>r f v u e h z p w w</i> ; |
| 4. <i>р б у ы м х к ф р н</i> ; | 14. <i>c p p q i h z l l w o d e</i> ; |
| 5. <i>н ё т т и т й н т ь х й ь</i> ; | 15. <i>o q g u e y o v v</i> ; |
| 6. <i>у р н с ц т к ф р н</i> ; | 16. <i>c b v h k t x f</i> ; |
| 7. <i>к п о т н й р ш х д у</i> ; | 17. <i>f v p f x t x</i> ; |
| 8. <i>д н у х д ч ф ю х ч ы э з</i> ; | 18. <i>h p o r x t v f</i> ; |
| 9. <i>г й с з ф ф с х ц у ш ь ю и</i> ; | 19. <i>d j o h r x o v v</i> ; |
| 10. <i>п с ж с е х ё о ц к й ш ф с</i> ; | 20. <i>g p q v i g k y z h</i> . |

Задание 5

Зашифровать шифром Белазо сообщение на данном ключе:

- | | |
|--|------------------------------------|
| 1. <i>orientable surface</i> ; | ключ: <i>factor</i> ; |
| 2. <i>vector field</i> ; | ключ: <i>manifold</i> ; |
| 3. <i>Euler characteristic</i> ; | ключ: <i>surface</i> ; |
| 4. <i>cotangent bundle</i> ; | ключ: <i>category</i> ; |
| 5. <i>vector field</i> ; | ключ: <i>functor</i> ; |
| 6. <i>vector space</i> ; | ключ: <i>problem</i> ; |
| 7. <i>cellular structure</i> ; | ключ: <i>axiomatics</i> ; |
| 8. <i>critical point</i> ; | ключ: <i>absence</i> ; |
| 9. <i>critical value</i> ; | ключ: <i>technique</i> ; |
| 10. <i>chain complex</i> ; | ключ: <i>vector</i> ; |
| 11. <i>линейное пространство</i> ; | ключ: <i>вектор</i> ; |
| 12. <i>ориентируемая поверхность</i> ; | ключ: <i>базис</i> ; |
| 13. <i>клеточный комплекс</i> ; | ключ: <i>проекция</i> ; |
| 14. <i>критическое значение</i> ; | ключ: <i>инверсия</i> ; |
| 15. <i>характеристика кольца</i> ; | ключ: <i>транспозиция</i> ; |
| 16. <i>клеточный комплекс</i> ; | ключ: <i>перестановка</i> ; |
| 17. <i>информационная безопасность</i> ; | ключ: <i>теорема</i> ; |
| 18. <i>компьютерные науки</i> ; | ключ: <i>следствие</i> ; |
| 19. <i>мандатная политика</i> ; | ключ: <i>правило</i> ; |
| 20. <i>угроза безопасности</i> ; | ключ: <i>предел</i> . |

Задание 6

Расшифровать сообщение, зашифрованное шифром Белазо на данном ключе:

- | | |
|---------------------------------|--------------------|
| 1. ятпугёцаку нкднпсюжсгнрцаъ; | ключ: равенство; |
| 2. кияыбьбфняеюёуй зихзбыжжис; | ключ: замыкание; |
| 3. ькмёял юниасфрт; | ключ: квадрат; |
| 4. цффришоэчийюас рёёчг; | ключ: отрезок; |
| 5. ьютжсюфьфдйщопыач хтвуоццйы; | ключ: уравнение; |
| 6. ьохоутжб ардюгалотфжц; | ключ: касательная; |
| 7. трхэя пыушопй ьоюзита; | ключ: замыкание; |
| 8. пьтмфдыщудипн фсгвпбъхми; | ключ: тождество; |
| 9. ьрлгбавчгмря дэьлр; | ключ: поляра; |
| 10. ьэтмхчьу ббаярцгёньгеюю; | ключ: поверхность; |
| 11. fwfvqcfwhw pihrqcr; | ключ: discipline; |
| 12. jxhetbwbnr vyrakivplna; | ключ: education; |
| 13. vcgoitxfnjrp etdvwuyy ; | ключ: subject; |
| 14. sjkyqrroc aciqr; | ключ: opinion; |
| 15. ltsckf fhrwwmek; | ключ: theory; |
| 16. sxusuy fuyixjfn; | ключ: algebra; |
| 17. weioqrwmvt oes; | ключ: device; |
| 18. gmxxhvztgbwno shgiihz; | ключ: description; |
| 19. voaiicm xspvsg; | ключ: concept; |
| 20. hfrqre tvldgre; | ключ: example. |

Задание 7

Зашифровать сообщение шифром де ла Порта на данном ключе:

- | | |
|--------------------|-----------------|
| 1. comprehensible; | ключ: separate; |
| 2. knowledge; | ключ: further; |
| 3. preference; | ключ: lecture; |
| 4. experience; | ключ: deliver; |
| 5. researcher; | ключ: student; |
| 6. application; | ключ: reader; |
| 7. seminar; | ключ: author; |
| 8. attention; | ключ: revise; |
| 9. introduce; | ключ: drawing; |
| 10. surface; | ключ: chapter; |
| 11. tension; | ключ: show; |
| 12. deliberate; | ключ: lecture; |
| 13. indignation; | ключ: secret; |
| 14. inexpressive; | ключ: stain; |
| 15. unscrupulous; | ключ: stable; |
| 16. imperfect; | ключ: guardian; |
| 17. spontaneity; | ключ: remote; |
| 18. sympathy; | ключ: lapel; |
| 19. spectacles; | ключ: stick; |
| 20. panorama; | ключ: ward. |

Задание 8

Расшифровать сообщение, зашифрованное шифром де ла Porta на данном ключе:

1. *n g h o c p s l z t*; **ключ:** *sequence*;
2. *r z k u h k o s g b*; **ключ:** *compute*;
3. *f a o a s k g m*; **ключ:** *relation*;
4. *n n h t p f s f d*; **ключ:** *subject*;
5. *x b i d y n x f p u z x*; **ключ:** *objective*;
6. *l o a c t z a*; **ключ:** *number*;
7. *i a r h r l i u g b*; **ключ:** *variant*;
8. *u x x z y h x z k*; **ключ:** *singular*;
9. *s t d z y l t z l p*; **ключ:** *exercise*;
10. *i t e o r l x q*; **ключ:** *section*;
11. *z m u r g t m z f e*; **ключ:** *person*;
12. *d b d g d p l z s*; **ключ:** *garnet*;
13. *o e m l e y r l m l k*; **ключ:** *fuse*;
14. *x k l k w x f x x*; **ключ:** *spoil*;
15. *w h g p k b n t f*; **ключ:** *play*;
16. *m c n e f t k s p a l x x*; **ключ:** *peasant*;
17. *s n l b s z r b z*; **ключ:** *pilot*;
18. *z k g g f g d m*; **ключ:** *litre*;
19. *z k u r p w x*; **ключ:** *fiction*;
20. *g p s k t f m m*; **ключ:** *licence*;
21. *x n d r f e x q n*; **ключ:** *stripe*;
22. *w w g q y c o m u b*; **ключ:** *charge*;
23. *k t l n c g t o p c x*; **ключ:** *horizon*;
24. *q p d a c t m r w*; **ключ:** *prudence*;
25. *s g u a x s s u q x*; **ключ:** *unlike*;
26. *p e q m e x n y k x u t s*; **ключ:** *order*;
27. *m t w z t u t h p p*; **ключ:** *delay*;
28. *z x e o r p q t m e*; **ключ:** *piece*;
29. *h t e e m w r g y i w*; **ключ:** *peach*;
30. *d y o n q p y c*; **ключ:** *clerk*.

Задание 9

Зашифровать шифром на основе таблицы Виженера на данном ключе следующее сообщение:

1. векторное произведение; **ключ:** *странник*;
2. ориентированный объём; **ключ:** *оранжерей*;
3. каноническое разложение; **ключ:** *сервант*;
4. дискретное логарифмирование; **ключ:** *огурец*;
5. индекс инерции; **ключ:** *минор*;
6. смешанное произведение; **ключ:** *мангуст*;
7. эрмитова матрица; **ключ:** *дефект*;
8. базисный минор; **ключ:** *степень*;
9. направленный отрезок; **ключ:** *асимптота*;
10. собственное значение; **ключ:** *гипербола*;
11. вращать корнями; **ключ:** *ярлык*;
12. гусей дразнить; **ключ:** *молния*;
13. зарубить на носу; **ключ:** *кнопка*;
14. играть с огнём; **ключ:** *туман*;

- | | |
|----------------------------------|-------------------|
| 15. капля в море; | ключ: удочка; |
| 16. dynamic system; | ключ: receive; |
| 17. simple line of reasoning; | ключ: contribute; |
| 18. department of algebra; | ключ: edition; |
| 19. revised edition; | ключ: notion; |
| 20. systematic study; | ключ: purpose; |
| 21. mathematical discipline; | ключ: prepare; |
| 22. generally believed; | ключ: reader; |
| 23. geometric representation; | ключ: solution; |
| 24. attempt to formulate; | ключ: formation; |
| 25. higher order; | ключ: manifold; |
| 26. avec un grincement; | ключ: island; |
| 27. mettre les points sur les i; | ключ: remainder; |
| 28. vieux comme le monde; | ключ: negligence; |
| 29. construire sur le sable; | ключ: society; |
| 30. compter les corneilles; | ключ: injustice. |

Задание 10

Расшифровать сообщение, зашифрованное шифром Виженера на данном ключе:

- | | |
|---------------------------------|-----------------------|
| 1. лпэюепфщанаъов уяъэяаекмх; | ключ: икосаэдр; |
| 2. ххуазбъееньэяй в дээйьккащй; | ключ: треугольник; |
| 3. тхчфстащамюкшъ кмчт юб; | ключ: призма; |
| 4. фвылфпунэ тбоюяааюсюну; | ключ: параллелограмм; |
| 5. эуюьикиргтнх ввогбхн; | ключ: тетраэдр; |
| 6. явъъвимфдыёы кдяёьыс; | ключ: функция; |
| 7. охувщъьвё ычрщцнкгд; | ключ: кривизна; |
| 8. паэчдчмвчнцнн ыяуьидчл; | ключ: полином; |
| 9. уьясцгаюспаев филлютспр; | ключ: интеграл; |
| 10. гияччьец зсфцандогей; | ключ: частное; |
| 11. мьфужщтз мь уйоягъ унюйрщя; | ключ: интеграл; |
| 12. орлжрз ьеьня; | ключ: квадрика; |
| 13. стнён ю ыьдр ьэрвхё; | ключ: конус; |
| 14. цнгн ьех аи дуыпняф; | ключ: перспектива; |
| 15. трйвс д тюзаиъ; | ключ: крапива; |
| 16. ciavvufoqxi crikgtt; | ключ: advice; |
| 17. cettlеufx jrlghpj; | ключ: useful; |
| 18. zsmрсq aj vhhhsskf; | ключ: method; |
| 19. ysyokygc fhvyic; | ключ: remark; |
| 20. llfnfnhrgc asjrheiy; | ключ: graduate; |
| 21. ysyocyxc fhvyic; | ключ: remark; |
| 22. fcyqpzрсmт lfzixpkr; | ключ: number; |
| 23. evmenxrvpoc mitjuifni; | ключ: chapter; |
| 24. vonqtuxljul tkwnn; | ключ: quantity; |
| 25. qfsrk arjgmfrva; | ключ: misprint; |
| 26. iiagi jgzhu lm geey; | ключ: dispersion; |
| 27. vwjhzu hvv tsbxhw; | ключ: disorder; |
| 28. edeeyk tsf sfu; | ключ: execution; |
| 29. urmtm am vibgw; | ключ: precipice; |
| 30. reripv wlrs zy ghcts szmk; | ключ: leaflet. |

Задание 11

Зашифровать сообщение самоключом Виженера с данной начальной буквой « · »:

1. «v»; *to establish a connection;*
2. «x»; *in order to prove;*
3. «w»; *to bear in mind;*
4. «q»; *intuitive ideas;*
5. «t»; *corroborate strictly;*
6. «g»; *combinatorial topology;*
7. «i»; *task of generalizing;*
8. «n»; *impact on the investigation;*
9. «o»; *real variable;*
10. «r»; *general definition;*
11. «f»; *clair comme le jour;*
12. «q»; *on peut se casser la langue;*
13. «j»; *plaisanterie a part;*
14. «e»; *cousu avec du fil blanc;*
15. «z»; *gratter la langue;*
16. «p»; *прямоугольная матрица;*
17. «g»; *невыврожденная матрица;*
18. «ж»; *квадратная матрица;*
19. «з»; *невыврожденный оператор;*
20. «с»; *обратная матрица;*
21. «й»; *линейный функционал;*
22. «o»; *алгебраическое дополнение;*
23. «л»; *некоммутативная группа;*
24. «д»; *оператор проектирования;*
25. «к»; *положительное число;*
26. «х»; *устраивать сцену;*
27. «й»; *уносить ноги;*
28. «р»; *умывать руки;*
29. «д»; *уйти с головой;*
30. «э»; *ударить по рукам.*

Задание 12

Расшифровать сообщение, зашифрованное самоключом Виженера с начальной буквой « · »:

1. «в»; *я и р с с т а я м т г щ я с;*
2. «х»; *л я у ц ф а ь ц ь к я в у д г я п;*
3. «ч»; *и б ю а а п р ю а д г я у т ц з;*
4. «н»; *к и р с с т а в ю ь к;*
5. «ё»; *ж б з р ь я и а ж ж п э б я л;*
6. «л»; *п т ю ю ь щ ц ы ч р з ь ю ф ю т у а я а д г р н я д ф р;*
7. «д»; *д л о з ё с р и а ь ц ь к я н ю ф х р ц я з;*
8. «ш»; *г к н ь ь ц а ь ц ь у т л к м;*
9. «р»; *ы щ ь з т е ы ь ь с с ё г р т ь р;*
10. «м»; *ы ю ф х р т б я ф м э и щ х х т д я щ я р в н ц з;*
11. «к»; *л п ь з ь ь ш л р ю а я а;*
12. «м»; *н ь н о й т п щ т ё р я д;*
13. «п»; *с г ь к в т о ж ц ф ц;*
14. «д»; *ё й ж с о э ь ё к з з р я с г;*

15. «ф»; *цэжрчччо ю фзѠфф*;
16. «d»; *lubdfktn g vqbpgti*;
17. «h»; *wgftti hq walsfp*;
18. «k»; *lsrnpj yvwwertj*;
19. «j»; *lqbfa l hvr b m p mvsqfy r p g*;
20. «l»; *ohzzpzdbqrg ht flrkfsr*;
21. «f»; *vkultbttbdz tgfdtvkbmw*;
22. «p»; *glvcfv sblwzcb*;
23. «s»; *vlnkjvvr g kv tatkcs*;
24. «e»; *sputivrh ds s rvwmfe*;
25. «m»; *emvuep tgfdtvkr*;
26. «i»; *mrstbpgv lhr tdfkx sipzv kx*;
27. «s»; *jfabgv ppw dlnpgw*;
28. «d»; *dgo bxv cl mmiv*;
29. «r»; *jwvmdkg vvrqx jpr lh bilj*;
30. «c»; *oqwmlw r ss thwaw*.

Задание 13

Зашифровать сообщение обобщённым шифром Цезаря ($y \equiv x + \alpha \pmod{n}$):

- | | |
|---|---|
| 1. $\alpha = 4$; <i>singular</i> ; | 16. $\alpha = 23$; <i>пространство</i> ; |
| 2. $\alpha = 9$; <i>simplicial</i> ; | 17. $\alpha = 14$; <i>изоморфизм</i> ; |
| 3. $\alpha = 10$; <i>cellular</i> ; | 18. $\alpha = 31$; <i>коммутативность</i> ; |
| 4. $\alpha = 11$; <i>application</i> ; | 19. $\alpha = 28$; <i>дистрибутивность</i> ; |
| 5. $\alpha = 15$; <i>invigorate</i> ; | 20. $\alpha = 26$; <i>ассоциативность</i> ; |
| 6. $\alpha = 16$; <i>separate</i> ; | 21. $\alpha = 12$; <i>гомеоморфизм</i> ; |
| 7. $\alpha = 17$; <i>drawing</i> ; | 22. $\alpha = 7$; <i>подмножество</i> ; |
| 8. $\alpha = 19$; <i>gratitude</i> ; | 23. $\alpha = 25$; <i>факторгруппа</i> ; |
| 9. $\alpha = 21$; <i>discussion</i> ; | 24. $\alpha = 20$; <i>приближение</i> ; |
| 10. $\alpha = 22$; <i>purpose</i> ; | 25. $\alpha = 13$; <i>инвариантность</i> ; |
| 11. $\alpha = 5$; <i>applicant</i> ; | 26. $\alpha = 10$; <i>пропагандист</i> ; |
| 12. $\alpha = 7$; <i>prophecy</i> ; | 27. $\alpha = 15$; <i>знаменитость</i> ; |
| 13. $\alpha = 12$; <i>surface</i> ; | 28. $\alpha = 16$; <i>краситель</i> ; |
| 14. $\alpha = 13$; <i>panther</i> ; | 29. $\alpha = 19$; <i>растворитель</i> ; |
| 15. $\alpha = 18$; <i>organization</i> ; | 30. $\alpha = 9$; <i>диффеоморфизм</i> . |

Задание 14

Расшифровать сообщение, зашифрованное обобщённым шифром Цезаря:

1. $\alpha = 11$; *щъынопцуэпцж*;
2. $\alpha = 25$; *бёкэизжѠчобч*;
3. $\alpha = 15$; *яоцъэхуъчу*;
4. $\alpha = 10$; *юйфъштсйати*;
5. $\alpha = 27$; *йкщжинэиёцзге*;
6. $\alpha = 23$; *ёжеяюшыъыдяы*;
7. $\alpha = 18$; *атащясичяъц*;
8. $\alpha = 32$; *йнппджюхзю*;
9. $\alpha = 26$; *июйюклщжзыѠц*;
10. $\alpha = 16$; *уюяюыэфэшф*;
11. $\alpha = 16$; *пвьюбѠфан*;

12. $\alpha = 17$; *а я т х б ё ю я в з м*;
13. $\alpha = 21$; *в ф я з ц ф а р в у*;
14. $\alpha = 24$; *о ь д ж а ё е ч й*;
15. $\alpha = 9$; *ч ф с х ш с и м и*;
16. $\alpha = 5$; *k z s h y t w*;
17. $\alpha = 12$; *p q e o d u b f u a z*;
18. $\alpha = 12$; *o l w c a o h w q*;
19. $\alpha = 8$; *q v d i z q i v k m*;
20. $\alpha = 6$; *i g r i a r g z o u t*;
21. $\alpha = 18$; *w i m s d a l q*;
22. $\alpha = 24$; *g l r p m b s a r g m l*;
23. $\alpha = 20$; *x y p y f i j g y h n*;
24. $\alpha = 7$; *a l j o u p x b l*;
25. $\alpha = 13$; *g r e z v a b y b t l*;
26. $\alpha = 4$; *g s y r x i v t e r i*;
27. $\alpha = 9$; *y a x c n l c x a*;
28. $\alpha = 10$; *m y x d b y f o b c i*;
29. $\alpha = 11$; *x t o y t r s e*;
30. $\alpha = 15$; *t c r d j g p v t b t c i*.

Задание 15

Зашифровать сообщение поточным аффинным шифром простой замены
 $(y = E(x) \equiv \alpha x + \beta \pmod{n})$:

1. $\alpha = 11, \beta = 2$; *introduction*;
2. $\alpha = 23, \beta = 6$; *contractible*;
3. $\alpha = 9, \beta = 10$; *combinatorial*;
4. $\alpha = 15, \beta = 8$; *approximation*;
5. $\alpha = 17, \beta = 3$; *triangulation*;
6. $\alpha = 3, \beta = 15$; *transform*;
7. $\alpha = 5, \beta = 17$; *distinguish*;
8. $\alpha = 7, \beta = 11$; *determine*;
9. $\alpha = 19, \beta = 9$; *correspond*;
10. $\alpha = 21, \beta = 6$; *operation*;
11. $\alpha = 25, \beta = 12$; *infection*;
12. $\alpha = 9, \beta = 14$; *desolation*;
13. $\alpha = 11, \beta = 4$; *overgrowth*;
14. $\alpha = 5, \beta = 18$; *expiration*;
15. $\alpha = 7, \beta = 16$; *execution*;
16. $\alpha = 2, \beta = 18$; *конечная сумма*;
17. $\alpha = 4, \beta = 15$; *ортогональное дополнение*;
18. $\alpha = 5, \beta = 22$; *направленный отрезок*;
19. $\alpha = 7, \beta = 23$; *аффинная система*;
20. $\alpha = 13, \beta = 6$; *система координат*;
21. $\alpha = 16, \beta = 9$; *ортонормированный базис*;
22. $\alpha = 17, \beta = 3$; *разложение по базису*;
23. $\alpha = 14, \beta = 7$; *прямая сумма*;
24. $\alpha = 10, \beta = 11$; *декартово произведение*;
25. $\alpha = 8, \beta = 12$; *линейная зависимость*;
26. $\alpha = 19, \beta = 4$; *снимать пенки*;

27. $\alpha = 20$, $\beta = 5$; белая ворона;
 28. $\alpha = 23$, $\beta = 8$; больной вопрос;
 29. $\alpha = 13$, $\beta = 10$; вешать нос;
 30. $\alpha = 8$, $\beta = 12$; взять слово.

Задание 16

Расшифровать сообщение, зашифрованное поточным аффинным шифром простой замены:

1. $\alpha = 7$, $\beta = 4$; *irvgahiuehiyr*;
2. $\alpha = 11$, $\beta = 6$; *cettychqdqhkr*;
3. $\alpha = 23$, $\beta = 3$; *erhvfetrqy*;
4. $\alpha = 21$, $\beta = 8$; *yqvwutobidfo*;
5. $\alpha = 3$, $\beta = 15$; *uopcrefozpunfc*;
6. $\alpha = 5$, $\beta = 14$; *ygbpibfcgbor*;
7. $\alpha = 9$, $\beta = 11$; *dhydgjrfhy*;
8. $\alpha = 15$, $\beta = 5$; *jhseafjevuvoveb*;
9. $\alpha = 17$, $\beta = 2$; *ipvswniacnigr*;
10. $\alpha = 19$, $\beta = 10$; *koowgkhi*;
11. $\alpha = 5$, $\beta = 11$; *sftlzyafs*;
12. $\alpha = 9$, $\beta = 12$; *gzbwjkrb*;
13. $\alpha = 7$, $\beta = 9$; *dkkdymtwntv*;
14. $\alpha = 15$, $\beta = 5$; *nmwnjefevhs*;
15. $\alpha = 3$, $\beta = 18$; *bsfbezkif*;
16. $\alpha = 8$, $\beta = 13$; *щубфчблтсбу зшйбьту*;
17. $\alpha = 5$, $\beta = 17$; *щхгрмфрл щюиграль*;
18. $\alpha = 4$, $\beta = 11$; *емфецебкщыбкж имеюхднж*;
19. $\alpha = 7$, $\beta = 15$; *ъээрщпльнмт оыыовон*;
20. $\alpha = 2$, $\beta = 20$; *цюрысёусцс трцкэырчушэклорцшл*;
21. $\alpha = 10$, $\beta = 3$; *нффзйъкгыкгщ ючфснфсыь*;
22. $\alpha = 13$, $\beta = 6$; *ёочццёщ ньгерзчщ*;
23. $\alpha = 20$, $\beta = 7$; *йчцйлзцхз мьнхнжпзццйдчх*;
24. $\alpha = 17$, $\beta = 10$; *бвюьргювбкйррчо бьжма*;
25. $\alpha = 25$, $\beta = 20$; *юдуфпуажуы оуапнбу*;
26. $\alpha = 16$, $\beta = 5$; *мыфрлж ьэятще*;
27. $\alpha = 10$, $\beta = 12$; *рэиаэдгде вщыц*;
28. $\alpha = 23$, $\beta = 8$; *щймнгчпо ф цюз*;
29. $\alpha = 8$, $\beta = 14$; *щ йкфз мвквы*;
30. $\alpha = 13$, $\beta = 16$; *ягалаэ иёоуг*.

Задание 17

Зашифровать сообщение шифром Плейфера на основе английского алфавита с добавлением символов . (точка), , (запятая), _ (пробел), : (двоеточие), помещённых в таблицу 5×6, используя систематическое перемешивание на данном ключе:

1. Euler characteristic; **ключ:** failure;
2. tangential map; **ключ:** fabulist;
3. rank of mapping; **ключ:** diamond;
4. direct product; **ключ:** nitrogen;
5. orientable surface; **ключ:** authority;
6. projective space; **ключ:** designer;

- | | |
|---------------------------------|--------------------------------|
| 7. <i>sincere gratitude;</i> | ключ: <i>abstract;</i> |
| 8. <i>topological methods;</i> | ключ: <i>tailor;</i> |
| 9. <i>valuable advice;</i> | ключ: <i>question;</i> |
| 10. <i>fundamental theorem;</i> | ключ: <i>sandwich;</i> |
| 11. <i>object lesson;</i> | ключ: <i>weather;</i> |
| 12. <i>fashion house;</i> | ключ: <i>youth;</i> |
| 13. <i>looking forward;</i> | ключ: <i>store;</i> |
| 14. <i>exert influence;</i> | ключ: <i>survival;</i> |
| 15. <i>become acquainted;</i> | ключ: <i>breakfast.</i> |

Расшифровать сообщение, зашифрованное шифром Плейфера на основе английского алфавита с добавлением символов . (точка), , (запятая), _ (пробел) , : (двоеточие) , помещённых в таблицу 5×6, используя систематическое перемешивание на данном ключе:

- | | |
|--|---------------------------------|
| 16. <i>n j r , q w i w j x r , x o . r g n w . i b c n ;</i> | ключ: <i>interval;</i> |
| 17. <i>p a s u d x y m a h : m t q d j d p w . ;</i> | ключ: <i>triumph;</i> |
| 18. <i>e r n i a e r n k t m h m l j q t k w h h t m : ;</i> | ключ: <i>argument;</i> |
| 19. <i>l t r t c . p a a t p o t a k y ;</i> | ключ: <i>authorship;</i> |
| 20. <i>l i a t d i k : c a g t a n i n n h ;</i> | ключ: <i>production;</i> |
| 21. <i>y g k w a j t g v t x m w l y u o g j w ;</i> | ключ: <i>biography;</i> |
| 22. <i>p e h r p w i f w z h i h c n d d z ;</i> | ключ: <i>aphorism;</i> |
| 23. <i>e k i p k e : m g , t k o u d . j i u . ;</i> | ключ: <i>banquet;</i> |
| 24. <i>e u h f j y c n t , h l . e o n i a ;</i> | ключ: <i>: inaction;</i> |
| 25. <i>d a g e c m i : t v y e c h d x ;</i> | ключ: <i>machinery;</i> |
| 26. <i>q j k . n . h o b j y n d u : n p d w . h o b j y f j h u . ;</i> | ключ: <i>justice;</i> |
| 27. <i>k o t c , i l b i f p h s e g t d f , i i y b a ;</i> | ключ: <i>ovation;</i> |
| 28. <i>b o c p m , b u x v m f v f d s v ;</i> | ключ: <i>publicity;</i> |
| 29. <i>r b x n z g x j o : n h g : h f a n g f f e ;</i> | ключ: <i>founder;</i> |
| 30. <i>p c j q g e g y s w r w q k b k ;</i> | ключ: <i>proverb.</i> |

Задание 18

Зашифровать сообщение, используя шифр Плейфера на основе 30-буквенного (без ё, й, ь) русского алфавита, помещённого в таблицу 5×6, с использованием систематического перемешивания на данном ключе:

- | | |
|--|----------------------------------|
| 1. <i>вещественное пространство;</i> | ключ: <i>поверхность;</i> |
| 2. <i>комплексное линейное пространство;</i> | ключ: <i>коника;</i> |
| 3. <i>выполненное исследование;</i> | ключ: <i>квадратура;</i> |
| 4. <i>величина направленного отрезка;</i> | ключ: <i>эллипсоид;</i> |
| 5. <i>закон дистрибутивности;</i> | ключ: <i>гиперboloид;</i> |
| 6. <i>логическая независимость;</i> | ключ: <i>оператор;</i> |
| 7. <i>характеристика поля;</i> | ключ: <i>функционал;</i> |
| 8. <i>математические объекты;</i> | ключ: <i>многочлен;</i> |
| 9. <i>результаты исследования;</i> | ключ: <i>изоморфизм;</i> |
| 10. <i>геометрический смысл;</i> | ключ: <i>додекаэдр;</i> |
| 11. <i>искать днем с огнем;</i> | ключ: <i>струна;</i> |
| 12. <i>иметь голову на плечах;</i> | ключ: <i>пятница;</i> |
| 13. <i>вынести на плечах;</i> | ключ: <i>жилетка;</i> |
| 14. <i>витать в облаках;</i> | ключ: <i>удочка;</i> |
| 15. <i>видно птицу по полету;</i> | ключ: <i>коврижка.</i> |

Расшифровать сообщение, зашифрованное шифром Плейфера на основе 30-буквенного (без ё, й, ь) русского алфавита, помещенного в таблицу 5×6, с использованием систематического перемешивания на данном ключе:

- | | |
|--|--------------------------|
| 16. ж в к ц д ж н р е а и ш ф п ц м т у и р; | ключ: операция; |
| 17. б у т м п л ж ш о п л г п л д с р и ц; | ключ: элемент; |
| 18. р ц ч ж ь у ц г ь ц м э м р ж п д п к т; | ключ: кольцо; |
| 19. о р х о б у с о л м ж п т л с и ц; | ключ: вектор; |
| 20. ь л и ф а б п ж м в в н с м р н г м н и ц; | ключ: множество; |
| 21. ц ж е ф ь л з у п ш м р к и г а е а п к а л; | ключ: формула; |
| 22. л я в т д о л д е ч ч ж т х и ц ж б ь ь л е и; | ключ: функция; |
| 23. л п и ч с ч е с е т г л з а з н ч к р м; | ключ: система; |
| 24. п е и п к с ь р ь н г м н ц л и ш; | ключ: природа; |
| 25. з б е г б и ж ы л в ж о в ю ф н; | ключ: разложение; |
| 26. г р ь ю г б э е ф ж т а г о; | ключ: пузырь ; |
| 27. с о т и р ц о б ж и р ц и в л у; | ключ: кнопка; |
| 28. ы к и б ш п к а э ш м к р с; | ключ: корыто; |
| 29. р с к г ж с к ш я д л ц т к ф ы; | ключ: звено; |
| 30. т у б в г и ц с н ф а о п ж в с н и х; | ключ: сервант. |

Задание 19

Зашифровать сообщение шифром Хилла, если ключом является матрица A:

- | | |
|--|---|
| 1. <i>useful remarks</i> ; | $A = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 10 & 5 \\ 2 & 6 & 5 \end{pmatrix};$ |
| 2. <i>function theory</i> ; | $A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 5 & 3 \\ 3 & 8 & 5 \end{pmatrix};$ |
| 3. <i>geometric representation</i> ; | $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 4 & 7 & 6 \end{pmatrix};$ |
| 4. <i>profound theory</i> ; | $A = \begin{pmatrix} 2 & 2 & 1 \\ 3 & 3 & 2 \\ 5 & 6 & 4 \end{pmatrix};$ |
| 5. <i>attempt to formulate</i> ; | $A = \begin{pmatrix} 1 & 5 & 1 \\ 3 & 14 & 2 \\ 2 & 9 & 2 \end{pmatrix};$ |
| 6. <i>requirements of the theory</i> ; | $A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 3 & 7 & 5 \end{pmatrix};$ |
| 7. <i>important concept</i> ; | $A = \begin{pmatrix} 5 & 4 & 3 \\ 4 & 3 & 3 \\ 9 & 7 & 7 \end{pmatrix};$ |
| 8. <i>branche of mathematics</i> ; | $A = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 7 & 5 \\ 4 & 9 & 10 \end{pmatrix};$ |
| 9. <i>considerable influence</i> ; | $A = \begin{pmatrix} 2 & 3 & 1 \\ 5 & 7 & 3 \\ 3 & 4 & 3 \end{pmatrix};$ |
| 10. <i>development of algebra</i> ; | $A = \begin{pmatrix} 3 & 2 & 2 \\ 4 & 3 & 3 \\ 6 & 5 & 4 \end{pmatrix};$ |

11. *конечное множество;*

$$A = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 2 & 3 & 3 & 2 \\ 1 & 3 & 5 & 2 \\ 4 & 5 & 5 & 5 \end{pmatrix};$$

12. *алгебраическая операция;*

$$A = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 2 & 3 & 4 & 2 \\ 1 & 2 & 3 & 2 \\ 3 & 5 & 7 & 5 \end{pmatrix};$$

13. *коммутативная операция;*

$$A = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 2 & 4 & 3 & 2 \\ 1 & 3 & 2 & 2 \\ 3 & 7 & 5 & 5 \end{pmatrix};$$

14. *свойство ассоциативности;*

$$A = \begin{pmatrix} 4 & 2 & 3 & 2 \\ 3 & 1 & 2 & 2 \\ 7 & 3 & 5 & 5 \\ 2 & 1 & 1 & 1 \end{pmatrix};$$

15. *отношение эквивалентности;*

$$A = \begin{pmatrix} 1 & 3 & 2 & 1 \\ 2 & 5 & 4 & 3 \\ 1 & 4 & 3 & 1 \\ 3 & 9 & 7 & 5 \end{pmatrix};$$

16. *непересекающиеся группы;*

$$A = \begin{pmatrix} 3 & 1 & 2 & 1 \\ 5 & 2 & 4 & 3 \\ 9 & 3 & 7 & 5 \\ 4 & 1 & 3 & 1 \end{pmatrix};$$

17. *классы эквивалентности;*

$$A = \begin{pmatrix} 3 & 4 & 2 & 5 \\ 5 & 7 & 3 & 9 \\ 1 & 2 & 1 & 3 \\ 1 & 3 & 1 & 4 \end{pmatrix};$$

18. *разбиение множества на классы;*

$$A = \begin{pmatrix} 1 & 1 & 3 & 2 \\ 3 & 2 & 5 & 4 \\ 4 & 2 & 6 & 5 \\ 4 & 3 & 8 & 7 \end{pmatrix};$$

19. *фундаментальное понятие;*

$$A = \begin{pmatrix} 1 & 1 & 3 & 2 \\ 3 & 2 & 5 & 4 \\ 4 & 2 & 6 & 5 \\ 4 & 3 & 8 & 7 \end{pmatrix};$$

20. *направленный отрезок;*

$$A = \begin{pmatrix} 3 & 2 & 1 & 1 \\ 5 & 4 & 2 & 3 \\ 6 & 5 & 2 & 4 \\ 8 & 7 & 3 & 4 \end{pmatrix};$$

21. *at the bottom of;*

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 4 \\ 1 & 4 & 6 \end{pmatrix};$$

22. *have influence;*

$$A = \begin{pmatrix} 1 & -1 & 3 \\ 0 & 4 & 5 \\ 2 & 1 & 4 \end{pmatrix};$$

23. *a matter of taste;*

$$A = \begin{pmatrix} 3 & 4 & 1 \\ 2 & 1 & 1 \\ 4 & 5 & 2 \end{pmatrix};$$

24. *make alterations;*

$$A = \begin{pmatrix} 5 & 3 & 2 \\ 4 & 1 & 3 \\ 2 & 2 & 3 \end{pmatrix};$$

25. *as quick as possible;*

$$A = \begin{pmatrix} 3 & 1 & 2 \\ 4 & 1 & 3 \\ 1 & 5 & 5 \end{pmatrix};$$

26. с больной головы на здоровую;

$$A = \begin{pmatrix} 4 & 3 & 3 & 3 \\ 1 & 2 & 2 & 1 \\ 1 & 1 & 2 & 1 \\ 2 & 3 & 4 & 3 \end{pmatrix};$$

27. без сучка без задоринки;

$$A = \begin{pmatrix} 1 & 1 & 0 & -1 \\ 2 & 3 & 1 & 0 \\ 3 & 4 & 2 & 1 \\ -1 & 2 & 1 & 2 \end{pmatrix};$$

28. блуждать в потёмках;

$$A = \begin{pmatrix} 2 & 1 & 3 & 2 \\ 1 & 0 & 2 & 1 \\ 3 & 1 & 6 & 3 \\ 6 & 2 & 10 & 8 \end{pmatrix};$$

29. брать с потолка;

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 1 & 2 & 2 \\ 1 & 1 & -1 & 2 \\ 3 & 2 & 1 & 5 \end{pmatrix};$$

30. бросать слова на ветер;

$$A = \begin{pmatrix} 2 & 1 & -1 & 3 \\ 3 & 2 & 0 & 2 \\ 5 & 3 & 1 & 5 \\ 4 & 2 & 2 & 7 \end{pmatrix}.$$

Задание 20

Расшифровать сообщение, зашифрованное шифром Хилла, если ключом является матрица A :

1. *uiwplp ourl yszuhhawodu,*

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 0 \\ 1 & 4 & 2 \end{pmatrix};$$

2. *mhcvdlbo zry ttykfltaqx,*

$$A = \begin{pmatrix} 1 & -1 & 1 \\ 2 & 3 & 1 \\ 3 & 4 & 1 \end{pmatrix};$$

3. *rkerrnp kg mvlmevzfr,*

$$A = \begin{pmatrix} 2 & 0 & 1 \\ 3 & 4 & 6 \\ -1 & 1 & 2 \end{pmatrix};$$

4. *qndli nnbjnusebghwk,*

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 1 & 1 \\ 3 & 0 & 4 \end{pmatrix};$$

5. *sgjgawo gwshtwc,*

$$A = \begin{pmatrix} 3 & 2 & 1 \\ 4 & 3 & 2 \\ 5 & 3 & 8 \end{pmatrix};$$

6. *uuwppp ixfwpangtib,*

$$A = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 4 & 1 \\ 4 & 7 & 2 \end{pmatrix};$$

7. *odujrbqtnc blezetfu,*

$$A = \begin{pmatrix} 3 & 2 & 4 \\ 4 & 1 & 5 \\ 6 & 4 & 7 \end{pmatrix};$$

8. *frv wwvzlnmsg ug kzrlphbcde,*

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & 3 & 6 \\ 5 & 4 & 7 \end{pmatrix};$$

9. *ttquks uqv mepwedhtn,*

$$A = \begin{pmatrix} 3 & 1 & 2 \\ 4 & 2 & 1 \\ 6 & 3 & 4 \end{pmatrix};$$

10. $abqnlzdzh\ uz\ pgwefkylgi,$ $A = \begin{pmatrix} 5 & 2 & 3 \\ 6 & 3 & 5 \\ 7 & 3 & 1 \end{pmatrix}.$
11. $тпмм юъдеищнпч,$ $A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 3 & 7 & 5 \end{pmatrix};$
12. $впъебэбрьгъреое,$ $A = \begin{pmatrix} 2 & 2 & 1 \\ 3 & 4 & 2 \\ 5 & 7 & 3 \end{pmatrix};$
13. $хиоюгнщнщифкчяя,$ $A = \begin{pmatrix} 3 & 5 & 1 \\ 4 & 6 & 2 \\ 7 & 12 & 3 \end{pmatrix};$
14. $йгнвгцьщдшзехуфжкъ,$ $A = \begin{pmatrix} 3 & 4 & 5 \\ 4 & 3 & 6 \\ 7 & 8 & 11 \end{pmatrix};$
15. $дзъухцшзеозевояъэъвъезйл,$ $A = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 7 & 4 \\ 3 & 10 & 7 \end{pmatrix};$
16. $аазялыэенишчъмфёдщйуфх,$ $A = \begin{pmatrix} 1 & 1 & 2 \\ 3 & 4 & 6 \\ 5 & 6 & 11 \end{pmatrix};$
17. $йдооцлнчмъбфнеы,$ $A = \begin{pmatrix} 2 & 1 & 1 \\ 3 & 1 & 2 \\ 5 & 3 & 3 \end{pmatrix};$
18. $фгёцъро ежсдликн,$ $A = \begin{pmatrix} 2 & 3 & 1 \\ 4 & 7 & 3 \\ 6 & 10 & 5 \end{pmatrix};$
19. $мшбхщътпофпаацъцитссъ,$ $A = \begin{pmatrix} 5 & 4 & 3 \\ 4 & 3 & 2 \\ 1 & 1 & 2 \end{pmatrix};$
20. $иаьщуяадюытнцжгрлеэои,$ $A = \begin{pmatrix} 6 & 1 & 3 \\ 7 & 2 & 6 \\ 5 & 2 & 4 \end{pmatrix};$
21. $pm\ wfk\ txyu\ no\ eskr gjrtp,$ $A = \begin{pmatrix} 1 & -1 & 3 \\ 0 & 4 & 5 \\ 2 & 1 & 4 \end{pmatrix};$
22. $ihwtdwym\ zwcm tviqgr,$ $A = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 3 & -1 \\ 3 & 4 & 4 \end{pmatrix};$
23. $wzy\ uojjm\ bu\ zllek,$ $A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \\ 5 & 6 & 8 \end{pmatrix};$
24. $glxdjiw\ eevjkcfbqgt,$ $A = \begin{pmatrix} 1 & 1 & 2 \\ 2 & 1 & 5 \\ 3 & 3 & 9 \end{pmatrix};$
25. $qhi\ romjw\ dxueqwk,$ $A = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 2 & 0 \\ 3 & 3 & 2 \end{pmatrix};$

26. *xxlumaujxkto zy lbqxsul*, $A = \begin{pmatrix} 3 & 1 & 1 \\ 2 & 1 & 1 \\ 5 & 2 & 3 \end{pmatrix};$
27. *attshn pxi lsn*, $A = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 0 & 1 \\ 4 & 2 & -1 \end{pmatrix};$
28. *asep mg irzpi b*, $A = \begin{pmatrix} 3 & 4 & 5 \\ 4 & 5 & 6 \\ 7 & 9 & 12 \end{pmatrix};$
29. *aglgoh lz uqgzora*, $A = \begin{pmatrix} 1 & -1 & 1 \\ 2 & 3 & 4 \\ 1 & 4 & 6 \end{pmatrix};$
30. *lyjs kr i ghcbhumtnse*, $A = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 7 & 6 \\ 4 & 9 & 11 \end{pmatrix}.$

Задание 21

Зашифровать двойным шифром Хилла сообщение на данных ключах А и В ($y = BAx$):

1. абелева группа, $A = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}, B = \begin{pmatrix} 9 & 2 \\ 5 & 1 \end{pmatrix};$
2. факториальное кольцо, $A = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}, B = \begin{pmatrix} 7 & 4 \\ 2 & 1 \end{pmatrix};$
3. достаточное условие, $A = \begin{pmatrix} 4 & 2 \\ 3 & 4 \end{pmatrix}, B = \begin{pmatrix} 7 & 2 \\ 6 & 5 \end{pmatrix};$
4. циклическая группа, $A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}, B = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix};$
5. цепная дробь, $A = \begin{pmatrix} 10 & 4 \\ 2 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & -1 \\ 2 & 3 \end{pmatrix};$
6. алгоритм Евклида, $A = \begin{pmatrix} 5 & 9 \\ 6 & 11 \end{pmatrix}, B = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix};$
7. коэффициенты Безу, $A = \begin{pmatrix} 4 & 3 \\ 5 & 4 \end{pmatrix}, B = \begin{pmatrix} 7 & 5 \\ 1 & 3 \end{pmatrix};$
8. расширенный алгоритм, $A = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}, B = \begin{pmatrix} 8 & 1 \\ 2 & 2 \end{pmatrix};$
9. оценка сложности, $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, B = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix};$
10. мультипликативная группа, $A = \begin{pmatrix} 5 & 11 \\ 2 & 4 \end{pmatrix}, B = \begin{pmatrix} 5 & 3 \\ 1 & 2 \end{pmatrix};$
11. необходимое условие, $A = \begin{pmatrix} 6 & 4 \\ 8 & 6 \end{pmatrix}, B = \begin{pmatrix} 3 & 5 \\ 4 & 6 \end{pmatrix};$
12. *most closely related to*, $A = \begin{pmatrix} 6 & 7 \\ 3 & 3 \end{pmatrix}, B = \begin{pmatrix} 8 & 3 \\ -1 & 3 \end{pmatrix};$
13. *fundamental course*, $A = \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}, B = \begin{pmatrix} -6 & 11 \\ -9 & 3 \end{pmatrix};$

14. <i>general applications,</i>	$A = \begin{pmatrix} 2 & -1 \\ 3 & 8 \end{pmatrix}, B = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix};$
15. <i>design one's own course,</i>	$A = \begin{pmatrix} 1 & 5 \\ 3 & -2 \end{pmatrix}, B = \begin{pmatrix} 7 & 5 \\ 4 & 3 \end{pmatrix};$
16. <i>to draw the attention,</i>	$A = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}, B = \begin{pmatrix} 3 & 1 \\ 4 & 5 \end{pmatrix};$
17. <i>number of devices,</i>	$A = \begin{pmatrix} 4 & 5 \\ 1 & 2 \end{pmatrix}, B = \begin{pmatrix} 11 & 2 \\ 4 & 1 \end{pmatrix};$
18. <i>in order to introduce,</i>	$A = \begin{pmatrix} 1 & 3 \\ 5 & 4 \end{pmatrix}, B = \begin{pmatrix} 1 & 2 \\ 3 & 7 \end{pmatrix};$
19. <i>constructive concepts,</i>	$A = \begin{pmatrix} 10 & 3 \\ 5 & 1 \end{pmatrix}, B = \begin{pmatrix} -1 & -3 \\ 4 & 5 \end{pmatrix};$
20. <i>notion of factor space,</i>	$A = \begin{pmatrix} 1 & 4 \\ 3 & 5 \end{pmatrix}, B = \begin{pmatrix} 1 & 3 \\ 1 & 8 \end{pmatrix};$
21. <i>as if nothing had happened,</i>	$A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}, B = \begin{pmatrix} 6 & 7 \\ 3 & 3 \end{pmatrix};$
22. <i>take oneself in hand,</i>	$A = \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix}, B = \begin{pmatrix} 7 & 5 \\ 3 & 2 \end{pmatrix};$
23. <i>pull oneself together,</i>	$A = \begin{pmatrix} 1 & 1 \\ -2 & 3 \end{pmatrix}, B = \begin{pmatrix} -1 & 4 \\ 1 & 1 \end{pmatrix};$
24. <i>withdraw one's words,</i>	$A = \begin{pmatrix} 2 & 7 \\ 1 & 5 \end{pmatrix}, B = \begin{pmatrix} -1 & 3 \\ 4 & 5 \end{pmatrix};$
25. <i>be in the limelight,</i>	$A = \begin{pmatrix} 3 & 1 \\ 3 & 2 \end{pmatrix}, B = \begin{pmatrix} 2 & 5 \\ 1 & 4 \end{pmatrix};$
26. <i>take into consideration,</i>	$A = \begin{pmatrix} 2 & -1 \\ 3 & 8 \end{pmatrix}, B = \begin{pmatrix} 3 & 1 \\ 4 & 5 \end{pmatrix};$
27. <i>draw attention,</i>	$A = \begin{pmatrix} 9 & 4 \\ -2 & 1 \end{pmatrix}, B = \begin{pmatrix} 8 & 3 \\ -1 & 3 \end{pmatrix};$
28. <i>to make responsible,</i>	$A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}, B = \begin{pmatrix} 9 & 1 \\ 7 & 2 \end{pmatrix};$
29. <i>lose an opportunity,</i>	$A = \begin{pmatrix} 6 & 7 \\ 3 & 5 \end{pmatrix}, B = \begin{pmatrix} 1 & -1 \\ 5 & 2 \end{pmatrix};$
30. <i>make a dream a reality,</i>	$A = \begin{pmatrix} 8 & 3 \\ 5 & 1 \end{pmatrix}, B = \begin{pmatrix} 8 & 3 \\ 3 & 2 \end{pmatrix}.$

Задание 22

Расшифровать сообщение, зашифрованное двойным шифром Хилла, если ключами являются матрицы А и В ($y = BAx$):

1. <i>t x z x x l i b q n a b q i w o y,</i>	$A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}, B = \begin{pmatrix} 2 & 3 \\ 1 & -2 \end{pmatrix};$
2. <i>c s w j b a f y h u u r k d u r,</i>	$A = \begin{pmatrix} 3 & 4 \\ 2 & 1 \end{pmatrix}, B = \begin{pmatrix} 2 & -1 \\ 3 & 8 \end{pmatrix};$
3. <i>w p u w n y m t q v y h e g r w,</i>	$A = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix}, B = \begin{pmatrix} 6 & 7 \\ 3 & 3 \end{pmatrix};$

4. *kixtcqvyswts natsskwi*, $A = \begin{pmatrix} 7 & 5 \\ 4 & 3 \end{pmatrix}, B = \begin{pmatrix} 8 & 3 \\ -1 & 3 \end{pmatrix};$
5. *iwtqaj jrjji en iyyvrnw*, $A = \begin{pmatrix} 2 & 1 \\ -3 & 4 \end{pmatrix}, B = \begin{pmatrix} 1 & 5 \\ 3 & -2 \end{pmatrix};$
6. *btr hhvuasgt jwdokzmub*, $A = \begin{pmatrix} 2 & 11 \\ 3 & 5 \end{pmatrix}, B = \begin{pmatrix} 3 & 1 \\ 4 & 7 \end{pmatrix};$
7. *kovzccb tbvgfidsu*, $A = \begin{pmatrix} 10 & 3 \\ 7 & 5 \end{pmatrix}, B = \begin{pmatrix} 3 & 1 \\ 4 & 7 \end{pmatrix};$
8. *umfsxwl syx btiuba*, $A = \begin{pmatrix} 7 & 3 \\ -2 & 5 \end{pmatrix}, B = \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix};$
9. *vtpnpa zaqiaxta*, $A = \begin{pmatrix} 11 & 2 \\ 4 & 1 \end{pmatrix}, B = \begin{pmatrix} 3 & 1 \\ -1 & 2 \end{pmatrix};$
10. *nemqm etkoe ov qggedmsx*, $A = \begin{pmatrix} 9 & 5 \\ 4 & 3 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix};$
11. *ucur chggzva jwxwpnnmr*, $A = \begin{pmatrix} 3 & 1 \\ 4 & 5 \end{pmatrix}, B = \begin{pmatrix} 4 & 5 \\ 1 & 2 \end{pmatrix};$
12. *щюхкмцмснкюят еънайеу*, $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, B = \begin{pmatrix} 5 & 3 \\ 1 & 2 \end{pmatrix};$
13. *йнабчттет хглэанрбдвщъмшгъэх*, $A = \begin{pmatrix} 4 & 3 \\ 5 & 4 \end{pmatrix}, B = \begin{pmatrix} 8 & 1 \\ 2 & 2 \end{pmatrix};$
14. *юъйлдиъи я вчкбтво*, $A = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}, B = \begin{pmatrix} 7 & 5 \\ 1 & 3 \end{pmatrix};$
15. *шынлффм вбзнщмвшыеч*, $A = \begin{pmatrix} 10 & 4 \\ 2 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix};$
16. *крбыдэжвш усуиъцг*, $A = \begin{pmatrix} 5 & 9 \\ 6 & 11 \end{pmatrix}, B = \begin{pmatrix} 1 & -1 \\ 2 & 3 \end{pmatrix};$
17. *оууцысцр уццхёцзы*, $A = \begin{pmatrix} 4 & 2 \\ 3 & 4 \end{pmatrix}, B = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix};$
18. *фроейтжцаг хвёлжюцтз*, $A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}, B = \begin{pmatrix} 7 & 2 \\ 6 & 5 \end{pmatrix};$
19. *лмкшчвоъцниу ёлечуяфф*, $A = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}, B = \begin{pmatrix} 9 & 2 \\ 5 & 1 \end{pmatrix};$
20. *дюоцжйсэ леълъчюр*, $A = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}, B = \begin{pmatrix} 7 & 4 \\ 2 & 1 \end{pmatrix};$
21. *sx tcw fwsz culyhyd*, $A = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}, B = \begin{pmatrix} 1 & -1 \\ 3 & 4 \end{pmatrix};$
22. *asrfpg rfb qzax bqytg*, $A = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 3 \\ 5 & 4 \end{pmatrix};$
23. *kv e ydyzd rigfanms*, $A = \begin{pmatrix} 3 & 1 \\ 4 & 5 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}.$
24. *fonsj ez vdqgyhs*, $A = \begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix}, B = \begin{pmatrix} -1 & 2 \\ 4 & 1 \end{pmatrix}.$
25. *vwbjk qlyd rmt ypoc*, $A = \begin{pmatrix} 5 & 2 \\ 3 & 1 \end{pmatrix}, B = \begin{pmatrix} 7 & 3 \\ 6 & 5 \end{pmatrix};$

26. *b g d s a r u k b e p u d s h f*, $A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 4 & 1 \\ 3 & 5 \end{pmatrix}$;
27. *x w e n w s l u c l o i m w q i i m j o*, $A = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 2 & -1 \\ 3 & 8 \end{pmatrix}$;
28. *t f q t f v k l j o e c m o*, $A = \begin{pmatrix} 3 & 1 \\ 4 & 7 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 5 \\ 3 & -2 \end{pmatrix}$;
29. *l v o h d a n h e a s t s p d d*, $A = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 3 \\ 1 & -2 \end{pmatrix}$;
30. *f g s p s q g m c g m s h i*, $A = \begin{pmatrix} 3 & 4 \\ 2 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & -1 \\ 2 & 1 \end{pmatrix}$.

Задание 23

Расшифровать сообщение, зашифрованное аффинным блочным шифром, если ключом являются матрица A и вектор b :

1. *p e v i v u y z d y s w w r z m n j j m g m d e*, $A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 4 \\ 1 & 4 & 6 \end{pmatrix}$, $b = \begin{pmatrix} 4 \\ 7 \\ 2 \end{pmatrix}$;
2. *f r b c r v s s e h v h i s x l v p h u r*, $A = \begin{pmatrix} 1 & -1 & 3 \\ 0 & 4 & 5 \\ 2 & 1 & 4 \end{pmatrix}$, $b = \begin{pmatrix} 2 \\ 5 \\ 3 \end{pmatrix}$;
3. *l v s s r c w o k y m d l l q o d c o y g*, $A = \begin{pmatrix} 3 & 4 & 1 \\ 2 & 1 & 1 \\ 4 & 5 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 11 \\ 8 \\ 5 \end{pmatrix}$;
4. *e m k z i e p c o z s g m k z*, $A = \begin{pmatrix} 5 & 3 & 2 \\ 4 & 1 & 3 \\ 2 & 2 & 3 \end{pmatrix}$, $b = \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix}$;
5. *d y t c y o r m g z l n c a z j s t j g j l s e r v x*, $A = \begin{pmatrix} 3 & 1 & 2 \\ 4 & 1 & 3 \\ 1 & 5 & 5 \end{pmatrix}$, $b = \begin{pmatrix} 8 \\ 9 \\ 3 \end{pmatrix}$;
6. *b k y u m u f l u n b g c s k*, $A = \begin{pmatrix} 2 & 1 & 2 \\ 1 & 2 & 1 \\ 3 & 8 & 8 \end{pmatrix}$, $b = \begin{pmatrix} 12 \\ 9 \\ 4 \end{pmatrix}$;
7. *u o u x h u a w g a g r f z t h u c*, $A = \begin{pmatrix} 5 & 1 & 1 \\ 1 & -2 & 2 \\ 4 & 1 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 18 \\ 1 \\ 7 \end{pmatrix}$;
8. *n e j h z a r b z i v q m i k z p s x y b*, $A = \begin{pmatrix} 9 & 4 & 1 \\ 3 & 5 & 2 \\ 1 & 2 & 4 \end{pmatrix}$, $b = \begin{pmatrix} 5 \\ 8 \\ 9 \end{pmatrix}$;
9. *t b v r o r g i p m t r t v z e v p p o t h y v*, $A = \begin{pmatrix} 7 & 3 & 2 \\ 6 & 4 & 1 \\ 2 & 3 & 3 \end{pmatrix}$, $b = \begin{pmatrix} 13 \\ 11 \\ 2 \end{pmatrix}$;
10. *c b w q q l k s d j h s p x s s m y*, $A = \begin{pmatrix} 5 & 3 & 2 \\ 4 & 2 & 3 \\ 9 & 6 & 6 \end{pmatrix}$, $b = \begin{pmatrix} 15 \\ 11 \\ 8 \end{pmatrix}$;

11. $aqmymlloxgir\ bso\ qssaocbvz,$ $A = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 3 \\ 7 & 6 & 9 \end{pmatrix}, b = \begin{pmatrix} 12 \\ 13 \\ 11 \end{pmatrix};$
12. $idcoabnxxzbl\ qdaum\ lkwiapk,$ $A = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 4 & 1 \\ 2 & 5 & 8 \end{pmatrix}, b = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix};$
13. $gsu\ fn\ elr\ ylxbddckvthei,$ $A = \begin{pmatrix} 3 & 2 & 1 \\ 4 & 1 & 1 \\ 5 & 2 & 10 \end{pmatrix}, b = \begin{pmatrix} 5 \\ 8 \\ 3 \end{pmatrix};$
14. $pwuiuymeu\ or\ kiipc\ duyutqjc,$ $A = \begin{pmatrix} 8 & 4 & 1 \\ 5 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix}, b = \begin{pmatrix} 12 \\ 15 \\ 3 \end{pmatrix};$
15. $esxkvayl\ bzmtyekxki\ tfrsr,$ $A = \begin{pmatrix} 7 & 3 & 2 \\ 6 & 5 & 1 \\ 3 & 3 & 1 \end{pmatrix}, b = \begin{pmatrix} 3 \\ 4 \\ 7 \end{pmatrix};$
16. $wbh\ ybqejdk\ pogxdsvlvd\ se\ jkcuhks,$ $A = \begin{pmatrix} 2 & 4 & 1 \\ 3 & 5 & 2 \\ 6 & 5 & 3 \end{pmatrix}, b = \begin{pmatrix} 4 \\ 5 \\ 2 \end{pmatrix};$
17. $mlbbon\ fp\ rohmjqogu\ ab\ k\ cvyufbf,$ $A = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 3 & 3 \\ 2 & 4 & 5 \end{pmatrix}, b = \begin{pmatrix} 4 \\ 3 \\ 6 \end{pmatrix};$
18. $dgz\ ntwfhavm\ dpjyrmtdosoqh\ hvcrck,$ $A = \begin{pmatrix} 1 & 4 & 5 \\ 3 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}, b = \begin{pmatrix} 8 \\ 3 \\ 5 \end{pmatrix};$
19. $hgmwmz\ yyallqhsyj\ tjvcl,$ $A = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 5 & 4 \\ 2 & 3 & 2 \end{pmatrix}, b = \begin{pmatrix} 3 \\ 4 \\ 6 \end{pmatrix};$
20. $nethadkx\ luol\ gbgxui,$ $A = \begin{pmatrix} 2 & 3 & 1 \\ 5 & 1 & 4 \\ 3 & 2 & 2 \end{pmatrix}, b = \begin{pmatrix} 17 \\ 13 \\ 10 \end{pmatrix};$
21. $llq\ dozklm\ iwzgx bmtz\ cqt,$ $A = \begin{pmatrix} 1 & 1 & 2 \\ 2 & 5 & 3 \\ 3 & 2 & 4 \end{pmatrix}, b = \begin{pmatrix} 3 \\ 4 \\ 7 \end{pmatrix};$
22. $omiprcr\ ir\ igvlcmoqzvco,$ $A = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 3 & 1 \\ 1 & 2 & 0 \end{pmatrix}, b = \begin{pmatrix} 8 \\ 5 \\ 11 \end{pmatrix};$
23. $ptdfyhz\ fd\ a\ ivxnhsvk,$ $A = \begin{pmatrix} 2 & 1 & -1 \\ 3 & 2 & 0 \\ 4 & 3 & 2 \end{pmatrix}, b = \begin{pmatrix} 6 \\ 1 \\ 9 \end{pmatrix};$
24. $vczbsxj\ gbabnmynedg,$ $A = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 5 & 4 \\ 4 & 11 & 7 \end{pmatrix}, b = \begin{pmatrix} 5 \\ 4 \\ 8 \end{pmatrix};$
25. $smw\ ertpibxlf\ urfaar,$ $A = \begin{pmatrix} 1 & 0 & -1 \\ 2 & 1 & 2 \\ 3 & 3 & -2 \end{pmatrix}, b = \begin{pmatrix} 3 \\ 11 \\ 4 \end{pmatrix};$
26. $mmk\ uglips\ awreabebb,$ $A = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 5 & 1 \\ 3 & 7 & 1 \end{pmatrix}, b = \begin{pmatrix} 9 \\ 13 \\ 4 \end{pmatrix};$

$$27. lotiiqtx \ qsyk \ h \ qnxgrg \ kuwiueej, \quad A = \begin{pmatrix} 2 & 1 & -1 \\ 3 & 1 & 7 \\ 2 & 1 & 2 \end{pmatrix}, \quad b = \begin{pmatrix} 8 \\ 5 \\ 16 \end{pmatrix};$$

$$28. ldigrs \ kq \ eaoufcwdzw, \quad A = \begin{pmatrix} 3 & 1 & 4 \\ 2 & 1 & 3 \\ 5 & 2 & 8 \end{pmatrix}, \quad b = \begin{pmatrix} 7 \\ 3 \\ 12 \end{pmatrix};$$

$$29. dbhlzqsp \ nicjgpf \ jojvey, \quad A = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 4 & 1 \\ 5 & 8 & 2 \end{pmatrix}, \quad b = \begin{pmatrix} 6 \\ 5 \\ 19 \end{pmatrix};$$

$$30. bo \ sm \ w \ dlimt \ sa \ havweptc \ pdhq, \quad A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 6 \\ 3 & 7 & 10 \end{pmatrix}, \quad b = \begin{pmatrix} 3 \\ 4 \\ 9 \end{pmatrix}.$$

Задание 24

Найти ключ аффинного блочного шифра, если известно, что данные 4 триграммы переводятся соответственно в 4 следующие за ними триграммы. Прочитать (расшифровать) криптограмму, зашифрованную на этом ключе:

1. *day,ecb,ebc,ecc; bgz,joo,ilm,koq;*
adiqe gcax umq mzy kdcfga ucv;
2. *but,cxv,dbw,cwv; ady,aqp,yff,bnl;*
ls jaho egs ndu wdmfm;
3. *put,qwu,rxu,srw; xfz,awu,cdu,gur;*
qekp mgga fcs gkb rlghhsx;
4. *cup,dwn,dvo,btr; bno,ipj,fpn,wmt;*
pz uqhcd fb bqjp mjrxkdgi;
5. *gun,ktm,dwm,hto; tgm,crv,nyv,vjw;*
pdfq gakvlnxa hu emfhvfaukr;
6. *map,mbo,tso,jdq; nza,pcf,cnw,rdl;*
ebbb fcohcrcm vkq zr ynerhws;
7. *top,wmn,ros,tpo; pjp,mjl,vqy,nfm;*
aqstj juzw evv frwrte jqa;
8. *dot,elv,foc,cqs; zmw,etd,ewr,wis;*
hfpchoq yiv ygxygwazbpiehj;
9. *ask,wuj,brm,bsj; muq,ahu,syb,nxs;*
gbqv ajzxps uck mf hfouqi;
10. *air,xet,ckq,zhs; pfp,ylk,asi,lbg;*
gdzps shnb zq zil vjeapqy;
11. *red,lxy,ofe,mge; wnc,kel,qpb,npa;*
xqrja pohz nau otavkvkqk;
12. *use,upg,wub,tsf; hae,xdc,wxi,dbd;*
ff djg saikpbgf x zj akyks;
13. *bar,ccp,cbq,azt; ymi,wlk,ymj,zok;*
dzzypdp alg nn lrjm yhbko;
14. *now,dqx,oov,rnx; usw,kba,ttz,bae;*
uq inpa cey gbof yba asvenlri;
15. *log,nof,gsf,lnh; rvt,tby,wll,wus;*
hetc huy inc dyjqcmdp;

16. *nap,ncm,pxr,mbp; eyl,rqy,tgz,bxj;
bnlian gmpg ri owlrx;*
17. *key,jux,ayx,slz; reg,dpg,fbd,yed;
wmnj ck vtjxsfxu snj;*
18. *net,eku,sbs,lfu; fip,inw,skz,aom;
zovkktfs vwqj pv fkc;*
19. *cap,gzo,zco,dzq; ogl,evj,xsv,wmq;
kumvvvz fe ywqmrupnz;*
20. *top,ulr,voo,sqo; fim,gce,ejm,fnt;
yb kvfpqfoc tslokqcc;*
21. *fog,gph,eoh,ask; cqa,idu,euh,ryb;
bo sm w dlimt sa havweptc pdhq;*
22. *new,pfu,ogl,let; oee,tms,led,hvo;
dbhlzqsp nicjgpf joivey;*
23. *one,que,put,lve; aek,npi,sgt,zgl;
ldigsr kq eaoufcwdzw;*
24. *let,map,ngu,ofv; ptc,rqs,uik,urn;
lotiiqtx qsyk h qnxgrg kuwiueej;*
25. *lit,mot,nus,pfs; itc,pzr,ucc,hje;
llq dozklm iwzgx bmtzcqt;*
26. *get,hot,ink,hgu; hwz,icu,asy,jfe;
omiprcr ir igvlcmoqzvco;*
27. *wet,vas,xhi,ksi; jxr,emz,zgi,kpp;
ptdfyhz fd aivxnhsvk;*
28. *sod,tij,upe,rqg; tsv,oob,afv.emi;
vczbsxj ghabnmynedg;*
29. *sec,tef,tfe,ufk; tdo.rll,skq,nyh;
smw ertpibxlf urfaar;*
30. *met,nfu,ogw,pix; kyj,mgu,npg,rcy;
mmk uglips awreabebbhj.*

Литература

1. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М. : Гелиос АРВ, 2001. 480 с.
2. Нечаев, В. И. Элементы криптографии. Основы теории защиты информации / В. И. Нечаев. – М. : Высшая школа, 1999. 109 с.
3. Введение в криптографию / под ред. В. В. Яценко. – М. : МЦНМО ЧеРо, 1998. 288 с.

Приложения

Таблица 1

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	21	22	23	24	25	26	27	28	29	30	31	32

Таблица 2

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

Таблица 3 (Третье)

[illegible]

Таблица 4 (Тритемия)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Таблица 5 (Виженера)

[illegible]

Таблица 6 (Виженера)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Таблица 7 (де ла Порта)

A	a	b	c	d	e	f	g	h	i	k	l	m
B	n	o	p	q	r	s	t	u	x	y	z	w
C	a	b	c	d	e	f	g	h	i	k	l	m
D	o	p	q	r	s	t	u	x	y	z	w	n
E	a	b	c	d	e	f	g	h	i	k	l	m
F	p	q	r	s	t	u	x	y	z	w	n	o
G	a	b	c	d	e	f	g	h	i	k	l	m
H	q	r	s	t	u	x	y	z	w	n	o	p
I	a	b	c	d	e	f	g	h	i	k	l	m
K	r	s	t	u	x	y	z	w	n	o	p	q
L	a	b	c	d	e	f	g	h	i	k	l	m
M	s	t	u	x	y	z	w	n	o	p	q	r
N	a	b	c	d	e	f	g	h	i	k	l	m
O	t	u	x	y	z	w	n	o	p	q	r	s
P	a	b	c	d	e	f	g	h	i	k	l	m
Q	u	x	y	z	w	n	o	p	q	r	s	t
R	a	b	c	d	e	f	g	h	i	k	l	m
S	x	y	z	w	n	o	p	q	r	s	t	u
T	a	b	c	d	e	f	g	h	i	k	l	m
U	y	z	w	n	o	p	q	r	s	t	u	x
X	a	b	c	d	e	f	g	h	i	k	l	m
Y	z	w	n	o	p	q	r	s	t	u	x	y
Z	a	b	c	d	e	f	g	h	i	k	l	m
W	w	n	o	p	q	r	s	t	u	x	y	z

Таблица 8 (де ла Порта)

A	a	b	c	d	e	f	g	h	i	j	k	l	m
B	n	o	p	q	r	s	t	u	v	w	x	y	z
C	a	b	c	d	e	f	g	h	i	j	k	l	m
D	o	p	q	r	s	t	u	v	w	x	y	z	n
E	a	b	c	d	e	f	g	h	i	j	k	l	m
F	p	q	r	s	t	u	v	w	x	y	z	n	o
G	a	b	c	d	e	f	g	h	i	j	k	l	m
H	q	r	s	t	u	v	w	x	y	z	n	o	p
I	a	b	c	d	e	f	g	h	i	j	k	l	m
J	r	s	t	u	v	w	x	y	z	n	o	p	q
K	a	b	c	d	e	f	g	h	i	j	k	l	m
L	s	t	u	v	w	x	y	z	n	o	p	q	r
M	a	b	c	d	e	f	g	h	i	j	k	l	m
N	t	u	v	w	x	y	z	n	o	p	q	r	s
O	a	b	c	d	e	f	g	h	i	j	k	l	m
P	u	v	w	x	y	z	n	o	p	q	r	s	t
Q	a	b	c	d	e	f	g	h	i	j	k	l	m
R	v	w	x	y	z	n	o	p	q	r	s	t	u
S	a	b	c	d	e	f	g	h	i	j	k	l	m
T	w	x	y	z	n	o	p	q	r	s	t	u	x
U	a	b	c	d	e	f	g	h	i	j	k	l	m
V	x	y	z	n	o	p	q	r	s	t	u	x	y
W	a	b	c	d	e	f	g	h	i	j	k	l	m
X	y	z	n	o	p	q	r	s	t	u	x	y	z
Y	a	b	c	d	e	f	g	h	i	j	k	l	m
Z	z	n	o	p	q	r	s	t	u	v	w	x	y

Оглавление

Введение.....	3
Исторические шифры замены.....	3
Шифр Цезаря.....	3
Шифр Тритемия.....	4
Шифр Белазо.....	5
Шифр де ла Порты.....	6
Шифр Виженера.....	7
Обобщенный шифр Цезаря.....	8
Аффинный поточный шифр.....	8
Блочные шифры простой замены.....	9
Шифр Плейфера.....	9
Шифр Хилла.....	10
Аффинный блочный шифр.....	13
Криптоатака.....	14
Задачи для самостоятельного решения.....	16
Литература.....	37
Приложения.....	38

Учебное издание

Яблокова Светлана Ивановна

**Задачи по криптографическим методам
защиты информации.
Симметричные криптосистемы**

Практикум

Редактор, корректор Л. Н. Селиванова
Компьютерная верстка Е. Б. Половкова

Подписано в печать 16.03.2020 Формат 60×84 1/8.
Усл. печ. л. 5,58. Уч.-изд. л. 2,0.
Тираж 3 экз. Заказ

Оригинал-макет подготовлен
в редакционно-издательском отделе
Ярославского государственного университета

Адрес типографии:
Ярославский государственный университет.
150003, Ярославль, ул. Советская, 14.

