Областное государственное бюджетное профессиональное образовательное учреждение

«СМОЛЕНСКАЯ АКАДЕМИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ»

Методическое пособие

для внеаудиторной самостоятельной работы студентов

по дисциплине «Криптографические методы защиты информации»

Смоленск 2015

Методическое пособие для внеаудиторной самостоятельной работы студентов по дисциплине «Криптографические методы защиты информации» для студентов первого курса специальности 090905 Организация и технология защиты информации (базовой подготовки).

Составитель: Малахова В.Г. – Смоленск: ОГБПОУ СмолАПО, 2015.

Методическое пособие ориентировано на формирование умений по расчету параметров типовых шифров замены и перестановки, использованию частотных характеристик языков в криптоанализе.

**СОДЕРЖАНИЕ**

[Пояснительная записка 4](#_Toc123855143)

[Тема «Основные понятия криптографии» 5](#_Toc123855144)

[Тема: «Криптоанализ шифра простой замены» 7](#_Toc123855145)

[Тема: «Простейшие методы шифрования с закрытым ключом» 10](#_Toc123855146)

[Тема: «Принципы построения блочных шифров с закрытым ключом» 18](#_Toc123855147)

[Тема: «Криптографические хеш-функции» 21](#_Toc123855148)

[Тема: «Поточные шифры и генераторы псевдослучайных чисел» 24](#_Toc123855149)

[Тема: «Поточные шифры и генераторы псевдослучайных чисел» 27](#_Toc123855150)

[Тема «Основные положения теории чисел, используемые в криптографии с открытым ключом» 33](#_Toc123855151)

[Тема «Криптографические алгоритмы с открытым ключом и их использование» 38](#_Toc123855152)

[Тема «Электронная цифровая подпись» 43](#_Toc123855153)

[Тема «Совершенно секретные системы» 46](#_Toc123855154)

[ПРИЛОЖЕНИЕ 1 51](#_Toc123855155)

[ПРИЛОЖЕНИЕ 2 58](#_Toc123855156)

[ПРИЛОЖЕНИЕ 3 59](#_Toc123855157)

[ПРИЛОЖЕНИЕ 4 60](#_Toc123855158)

[ПРИЛОЖЕНИЕ 5 61](#_Toc123855159)

# Пояснительная записка

Представленные материалы разработаны на основе рабочей программы учебной дисциплины «Криптографические методы защиты информации» для специальности среднего профессионального образования и предназначены для студентов 3 курса специальности 090905 Организация и технология защиты информации базовой подготовки.

Разработка имеет своей целью методическое сопровождение самостоятельной работы студентов по курсу дисциплины «Криптографические методы защиты информации» и ориентирована на формирование умений по расчету параметров типовых шифров замены и перестановки, использованию частотных характеристик языков в криптоанализе, а также общих компетенций по организации собственной деятельности, выбору типовых методов и способов выполнения профессиональных задач; использованию информационно-коммуникационных технологий, применению математического аппарата для решения профессиональных задач и профессиональных по организации документооборота, в том числе электронного, с учетом конфиденциальности информации, использованию нормативных правовых актов, нормативно-методических документов по защите информации.

Методические рекомендации охватывают все темы учебной дисциплины и содержат указания по выполнению заданий, список литературы.

В разработке указаны форма и порядок представления работы, сроки ее сдачи, критерии оценки работы.

«Лист самооценки» заполняется студентом с целью рефлексии проделанной работы.

# Тема «Основные понятия криптографии»

**Задание 1.** Зашифруйте слово ЗАМЕНА методом Цезаря.

***Методические рекомендации***

Шифр Цезаря применительно к русскому языку состоит в следующем. Каждая буква сообщения заменяется на другую, которая в русском алфавите отстоит от исходной на три позиции дальше.

Таким образом, буква A заменяется на Г, Б на Д и так далее вплоть до буквы Ь , которая заменялась на Я , затем Э на A , Ю на Б и, наконец, Я на В .

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Таким образом, слово ЗАМЕНА после шифрования методом Цезаря превратится в слово КГПЗРГ.

Это не очень сложный метод, тем более что при шифровании сообщений из нескольких слов сразу становится понятным, сколько слов содержал исходный текст. Кроме того, можно получить некоторую информацию по анализу повторов букв в зашифрованном сообщении. Например, в зашифрованном тексте КГПЗРГ одна из букв повторяется дважды. Тем не менее, Цезарь вошел в историю криптографии, а "шифр Юлия Цезаря", как его до сих пор называют, служит примером одной из первых систем шифрования.

Для расшифрования сообщения КГПЗРГ необходимо знать только сам алгоритм шифрования. Любой человек, знающий способ шифрования, легко может расшифровать секретное сообщение. Таким образом, ключом в данном методе является сам алгоритм.

**Задание 2.** Расшифруйте перехваченное секретное сообщение ЧСЮЭЮЪ. Противнику известно, что сообщение зашифровано шифром Цезаря, но ключ (параметр сдвига n) неизвестен и может принимать значения от 1 до 32.

***Методические рекомендации***

Известно, что буквы сдвигаются не на три знака вправо, а на n (0<n<33). В этом случае в системе шифрования появляется ключ – число n – параметр сдвига. Отправитель и получатель могут каким-либо образом договариваться (например, лично) и иногда менять значение ключа.

Известно, что перехвачено секретное сообщение ЧСЮЭЮЪ. Пытаясь найти значение секретного ключа, проведем атаку по шифртексту. Рассмотрим способ последовательного перебора всех возможных ключей (это так называемый метод "грубой силы").

Запишем на 32 строчках все варианты, которые получаются сдвигом каждой буквы на 1, 2, 3, ... , 32 позиции соответственно. Эту операцию можно проводить вручную, а можно составить несложную программу, которая запишет все варианты перебора параметра n в файл. Одна из этих 32 строк будет содержать исходное сообщение.

Таблица 1.1. Перебор вариантов для поиска ключа при использовании метода Цезаря для криптограммы ЧСЮЭЮЪ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | ШТЯЮЯЫ |  | 17 | ЗВОНОК |
| 2 | ЩУАЯАЬ |  | 18 | ИГПОПЛ |
| 3 | ЪФБАБЭ |  | 19 | ЙДРПРМ |
| 4 | ЫХВБВЮ |  | 20 | КЕСРСН |
| 5 | ЬЦГВГЯ |  | 21 | ЛЁТСТО |
| 6 | ЭЧДГДА |  | 22 | МЖУТУП |
| 7 | ЮШЕДЕБ |  | 23 | НЗФУФР |
| 8 | ЯЩЁЕЁВ |  | 24 | ОИХФХС |
| 9 | АЪЖЁЖГ |  | 25 | ПЙЦХЦТ |
| 10 | БЫЗЖЗД |  | 26 | РКЧЦЧУ |
| 11 | ВЬИЗИЕ |  | 27 | СЛШЧШФ |
| 12 | ГЭЙИЙЁ |  | 28 | ТМЩШЩХ |
| 13 | ДЮКЙКЖ |  | 29 | УНЪЩЪЦ |
| 14 | ЕЯЛКЛЗ |  | 30 | ФОЫЪЫЧ |
| 15 | ЁАМЛМИ |  | 31 | ХПЬЫЬШ |
| 16 | ЖБНМНЙ |  | 32 | ЦРЭЬЭЩ |

По таблице видно, что единственное слово, имеющее смысл, – это ЗВОНОК. Это слово располагается на 17 месте. Следовательно, если шифрованный текст сдвинуть на 17 позиций вперед получится открытый текст. Это означает, что для получения шифрованного текста открытый текст нужно сдвинуть на (33-17)=16 позиций. Таким образом, получили, что при шифровании использовался ключ n=16.

Так как ни при каком другом сдвиге не получилось осмысленного сообщения, то, скорее всего, мы правильно дешифровали это сообщение. Такое допущение о единственности решения вполне обоснованно, когда исходное сообщение составлено на одном из естественных языков (в рассмотренном примере – русском) и содержит более пяти-шести знаков. Но если сообщение очень короткое, возможных решений может быть несколько. Единственное решение также очень трудно найти, если исходное сообщение, состоит, например, из цифр.

**Задания для самостоятельного решения**

**1.** Определите ключи шифра Цезаря, если известны следующие пары открытый текст – шифротекст (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ):

а) АПЕЛЬСИН – ТВЧЮОДЫА б) МАНДАРИН – ТЁУЙЁЦОУ

**2.** Расшифруйте следующие сообщения, зашифрованные шифром Цезаря, и определите ключ n, 0<n<33, если известно, что исходные сообщения составлены из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ:

а) ЮВПЛШУХ б) СФЫЮБШЯФУ

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА:**

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных

**Интернет-ресурсы:**

www.intuit.ru

**Порядок представления материала:** на бумажном носителе или на сайте преподавателя.

**Срок представления материала:** семинарское занятие по теме.

**Форма контроля со стороны преподавателя:** собеседование

Критерии оценки: оценка «зачтено» ставится, если задачи решены правильно.

**ЛИСТ САМООЦЕНКИ**

|  |  |  |
| --- | --- | --- |
| Уровень освоения | Задание 1 | Задание 2 |
| Могу помочь другим |  |  |
| Выполнил без затруднений |  |  |
| Испытывал затруднения |  |  |

# Тема: «Криптоанализ шифра простой замены»

**Задание 1.** Дешифруйте текст, если известно, что зашифровано стихотворение Р. Киплинга в переводе С.Я. Маршака. Шифрование заключалось в замене каждой буквы на двузначное число. Отдельные слова разделены несколькими пробелами, знаки препинания сохранены. Таблица частот встречаемости букв русского языка приведена на .

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 29 | 15101729 | 222531153335 | 41434535 | 57 | 4525175915 | 10254125 |
| 69, | 597829 | 822578251715 | 10 | 88907825622522 | 1057737935 | 677890 |
| 8829453529, | 545790319073 | 228815882915 | 1769412515, | 7017905743 |  |  |
| 5915781562 | 222517572569 | 8815 | 82172588294535 |  |  |  |

***Методические рекомендации***

Криптоанализ шифра простой замены основан на использовании статистических закономерностей языка. Так, например, известно, что в русском языке частоты букв распределены следующим образом:

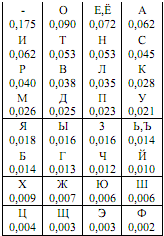


Рисунок 1 - Частоты букв русского языка (в 32-буквенном алфавите со знаком пробела)

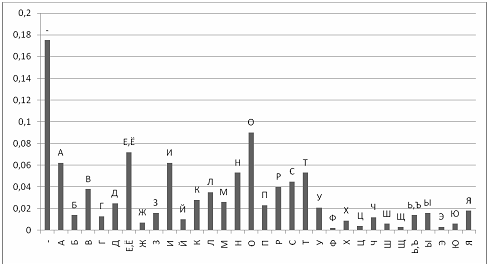


Рисунок 2 - Диаграмма частот букв русского языка

Для получения более точных сведений об открытых текстах можно строить и анализировать таблицы k-грамм при k>2, однако для учебных целей вполне достаточно ограничиться биграммами. Неравновероятность k -грамм (и даже слов) тесно связана с характерной особенностью открытого текста – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Так, для русского языка такими привычными фрагментами являются наиболее частые биграммы и триграммы:

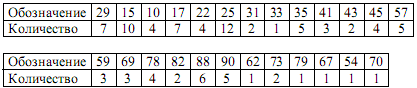
СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО,

СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА

Известно, что зашифровано стихотворение Р. Киплинга в переводе С.Я. Маршака. Шифрование заключалось в замене каждой буквы на двузначное число. Отдельные слова разделены несколькими пробелами и явно видны, знаки препинания сохранены. Таблица частот букв русского языка приведена выше.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 29 | 15101729 | 222531153335 | 41434535 | 57 | 4525175915 | 10254125 |
| 69, | 597829 | 822578251715 | 10 | 88907825622522 | 1057737935 | 677890 |
| 8829453529, | 545790319073 | 228815882915 | 1769412515, | 7017905743 |  |  |
| 5915781562 | 222517572569 | 8815 | 82172588294535 |  |  |  |

Подсчитаем частоты шифрообразований:



Из таблицы частот букв русского языка видно, что чаще всего встречается буква О, на втором месте Е. В нашем шифр-тексте чаще всего встречается обозначение 25 (12 раз), на втором месте идет обозначение 15 (10 раз), остальные обозначения им существенно уступают. Поэтому можем выдвинуть гипотезу: 25=О, 15=Е. Однако, текст у нас не очень большой, поэтому закономерности русского языка проявляются в нем не обязательно в строгом соответствии с таблицей частот букв русского языка. Поэтому возможен и вариант: 25=Е, 15=О. Но тогда последнее слово в третьей строке имеет окончание ЕО, что возможно, но все же более вероятный вариант ОЕ. Итак, будем работать с текстом, считая, что 25=О, 15=Е.

Теперь нам поможет знак препинания: «29, …». Крайне маловероятно, чтобы запятая стояла после согласной. Итак, 29 – гласная, причем вероятнее всего 29=И или 29=А, т.к. гласные Я, Ю, Э, У встречаются в осмысленных текстах на русском языке намного реже, чем И и А, что не противоречит таблице частот шифр-текста.

В последней строке: 88 15, но 15=Е, следовательно, 88 – согласная, причем наиболее вероятные значения – это Н и Т. Итак, 25=О, 15=Е, 29=А , 88=.

Теперь третье слово в третьей строке имеет 4 варианта:

29=И, 88=Н: 22 Н Е Н И Е

29=И, 88=Т: 22 Т Е Т И Е

29=А, 88=Н: 22 Н Е Н А Е

29=А, 88=Т: 22 Т Е Т А Е

Из рассмотренных вариантов лишь один является осмысленным, и он позволяет найти значение 22. Имеем: 22=М и третье слово в третье строке М Н Е Н И Е.

Теперь рассмотрим второе слово в первой строке. Е 10 17 И, причем 10 и 17 – согласные, и это не М и не Н. Наиболее вероятное слово Е С Л И, т.е. 10=С, 17=Л.

Конечно, если мы, продолжая работать с текстом, вдруг получим «нечитаемое» слово, то придется вернуться к этому этапу и рассмотреть другие варианты. Однако, это маловероятно, поскольку вряд ли в стихотворении были слова наподобие Е Р Т И, Е В Л И и т.п.

Далее, первое слово второй строки: 59 78 И, причем 59 и 78 – согласные, и это не С, не Л, не М и не Н. Так что это слово П Р И, т.е. 59=П, 78=Р. Тогда шестое слово первой строки 45 О Л П Е, что дает значение 45=Т и тогда при 57=В получаем фрагмент «…В Т О Л П Е…». Также второе слово последней строки П Е Р Е 62 дает нам значение 62=Д.

Далее рассмотрим начало второй строки: «П Р И 82 О Р О Л Е С Н 90 Р О Д О М …». Из него следует, что 82=К и 90=А.

Зная, что 82=К, посмотрим на самое последнее слово К Л О Н И Т 35, откуда станет ясно, что 35=Ь. Перед последней атакой выпишем текст, заменяя известные обозначения буквами.

И Е С Л И М О 31 Е 33 Ь 41 43 Т Ь В Т О Л П Е С О 41 О 69,

П Р И К О Р О Л Е С Н А Р О Д О М С В 73 79 Ь 67 Р А Н И Т Ь

И, 54 В А 31 А 73 М Н Е Н И Е Л 69 41 О Е,

70 Л А В 43 П Е Р Е Д М О Л В О 69 Н Е К Л О Н И Т Ь…

Из последней строки: 69=Ю, тогда слова Л Ю 41 О Е и С О 41 О Ю определяют 41: 41=Б. Теперь из четвертого слова первой строки Б 43 Т Ь получаем, что 43=Ы. А первое слово из последней строки 70 Л А В Ы – это Г Л А В Ы. Слово в первой строке М О 31 Е 33 Ь угадывается из контекста: М О Ж Е Ш Ь, т.е. 31=Ж, 33=Ш. Теперь второе слово в третьей строке запишется как 54 В А Ж А 73, откуда, с учетом контекста: 54=У, 73=Я. После этого окончание второй строки имеет вид «… С В Я 79 Ь 67 Р А Н И Т Ь». Легко определяются буквы 79=З, 67=Х.

Ответ:

И Е С Л И М О Ж Е Ш Ь Б Ы Т Ь В Т О Л П Е С О Б О Ю,

П Р И К О Р О Л Е С Н А Р О Д О М С В Я З Ь Х Р А Н И Т Ь

И, У В А Ж А Я М Н Е Н И Е Л Ю Б О Е,

Г Л А В Ы П Е Р Е Д М О Л В О Ю Н Е К Л О Н И Т Ь…

**Задания для самостоятельного решения**

**1.** Проведите статистический анализ теста и дешифруйте текст вашего варианта, который определяется номером по списку в журнале. При решении задачи можно воспользоваться помощью программы (взять у преподавателя). Данная программа предназначена для ускорения процесса по расчету частоты встречаемости символов в криптотексте, замене отдельных букв в криптотексте, предусмотрена возможность производить откат к предыдущему состоянию, если замена произведена неудачно.

Варианты шифротекста приведены в приложении 1.

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА:**

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных
2. Спирина М.С.,Спирин П.А.Дискретная математика:учебник: Рекомендовано ГОУВПО «МГТУ им. Н. Э. Баумана». — 9-e изд., испр. — 368 c., пер. No 7 бц.

**Интернет-ресурсы:**

www.intuit.ru

**Порядок представления материала:** на бумажном носителе или на сайте преподавателя.

**Срок представления материала:** семинарское занятие по теме.

**Форма контроля со стороны преподавателя:** собеседование

Критерии оценки: оценка «зачтено» ставится, если задачи решены правильно.

**ЛИСТ САМООЦЕНКИ**

|  |  |
| --- | --- |
| Уровень освоения | |
| Могу помочь другим |  |
| Выполнил без затруднений |  |
| Испытывал затруднения |  |

# Тема: «Простейшие методы шифрования с закрытым ключом»

**Задание 1.** Зашифруйте сообщение "ВЫШЛИТЕ ПОДКРЕПЛЕНИЕ" c использованием двух шифров ().

****

Рисунок 4 - Таблица замены для двух шифров простой замены: шифра №1 и шифра №2

***Методические рекомендации***

Одним из важных подклассов методов замены являются одноалфавитные (или моноалфавитные) подстановки, в которых устанавливается однозначное соответствие между каждым знаком ai исходного алфавита сообщений A и соответствующим знаком ei зашифрованного текста E.

В общем случае при одноалфавитной подстановке происходит однозначная замена исходных символов их эквивалентами из вектора замен (или таблицы замен). При таком методе шифрования ключом является используемая таблица замен ().

В таблице на самом деле объединены сразу две таблицы. Одна (шифр 1) определяет замену русских букв исходного текста на другие русские буквы, а вторая (шифр 2) – замену букв на специальные символы. Исходным алфавитом для обоих шифров будут заглавные русские буквы (за исключением букв "Ё" и "Й"), пробел и точка.

Зашифрованное сообщение с использованием любого шифра моноалфавитной подстановки получается следующим образом. Берется очередной знак из исходного сообщения. Определяется его позиция в столбце "Откр. текст" таблицы замен. В зашифрованное сообщение вставляется шифрованный символ из этой же строки таблицы замен.

Для шифрования берем первую букву исходного сообщения "В". В таблице на в столбце "Шифр 1" находим для буквы "В" заменяемый символ. Это будет буква "О". Записываем букву "О" под буквой "В".

|  |  |
| --- | --- |
| Рисунок 5 - Пример шифрования методом прямой замены | Затем рассматриваем второй символ исходного сообщения – букву "Ы". Находим эту букву в столбце "Откр. текст" и из столбца "Шифр 1" берем букву, стоящую на той же строке, что и буква "Ы".  Таким образом, получаем второй символ зашифрованного сообщения – букву "Н". |

Продолжая действовать аналогично, зашифровываем все исходное сообщение ().

**Задание 2.** Зашифруйте сообщение БОЛЬШОЙ СЕКРЕТ, используя пропорциональный шифр. Таблица замен приведена на .

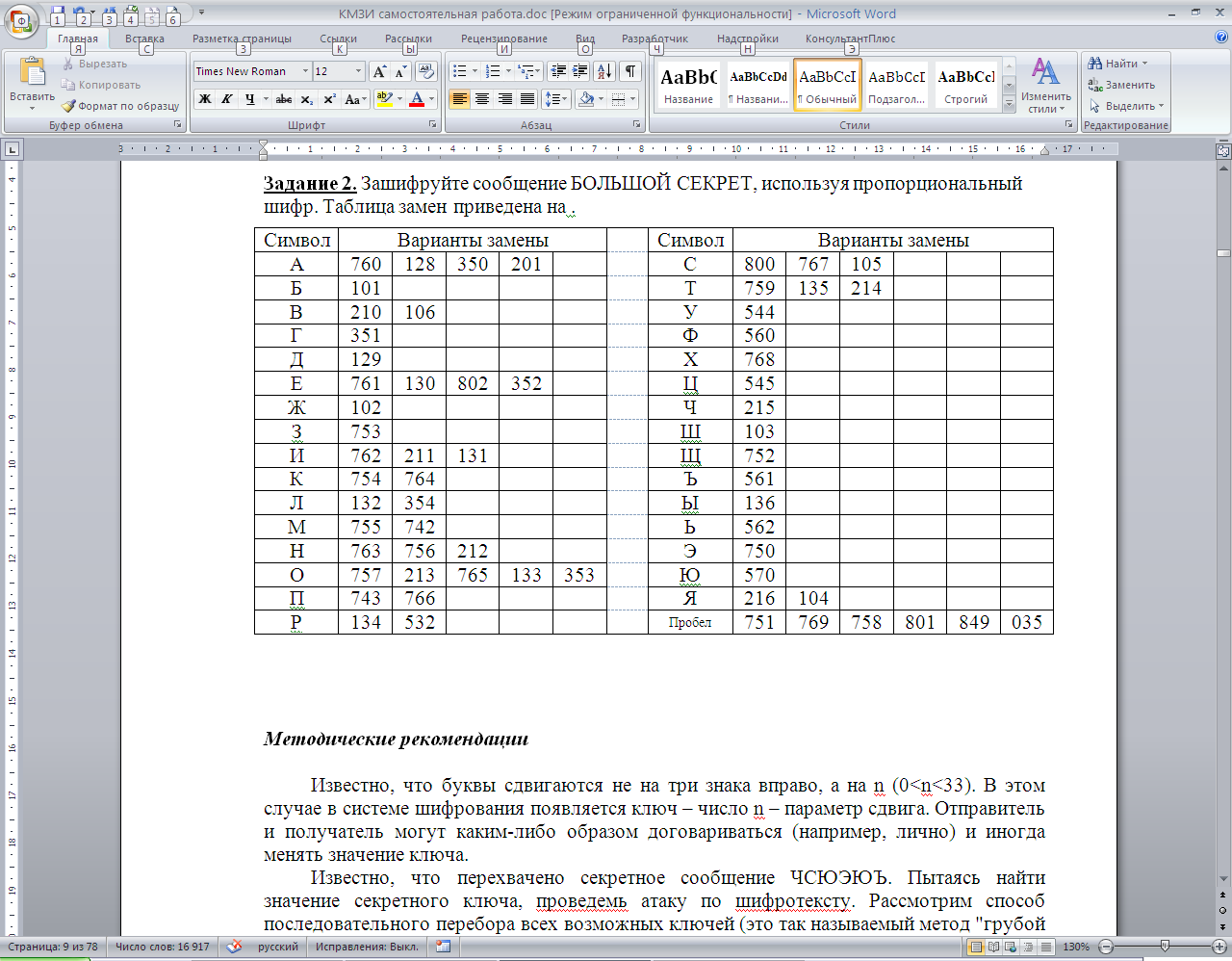


Рисунок 6 - Таблица замен

***Методические рекомендации***

В данном примере варианты замен для повторяющихся букв (например, "О") выбирались по порядку.

В этом случае сообщение может быть зашифровано следующим образом:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Б | О | Л | Ь | Ш | О | Й | пробел | С | Е | К | Р | Е | Т |
| 101 | 757 | 132 | 562 | 103 | 213 | 762 | 751 | 800 | 761 | 754 | 134 | 130 | 759 |

Интересно, что шифры, в которых производится замена букв несколькими символами, пропорционально встречаемости в открытом тексте, описывали итальянские ученые еще в XIV-XV веках.

Пропорциональные шифры более сложны для вскрытия, чем шифры простой одноалфавитной замены. Однако, если имеется хотя бы одна пара "открытый текст – шифротекст", вскрытие производится тривиально. Если же в наличии имеются только шифротексты, то вскрытие ключа, то есть нахождение таблицы замен, становится более трудоемким, но тоже вполне осуществимым.

**Задание 3.** Зашифруйте сообщение МЕТОД ПЕРЕСТАНОВКИ, используя шифр Виженера и ключ ВЕСНА.

***Методические рекомендации***

В целях маскирования естественной частотной статистики исходного языка применяется многоалфавитная подстановка. Примером многоалфавитной подстановки может служить схема, основанная на использовании таблицы Вижинера. Этот метод, известный уже в XVI веке, был описан французом Блезом Вижинером в "Трактате о шифрах", вышедшем в 1585 году.

В этом методе для шифрования используется таблица, представляющая собой квадратную матрицу с числом элементов NxN, где N — количество символов в алфавите (). В первой строке матрицы записывают буквы в порядке очередности их в исходном алфавите, во второй — ту же последовательность букв, но с циклическим сдвигом влево на одну позицию, в третьей — со сдвигом на две позиции и т. д.

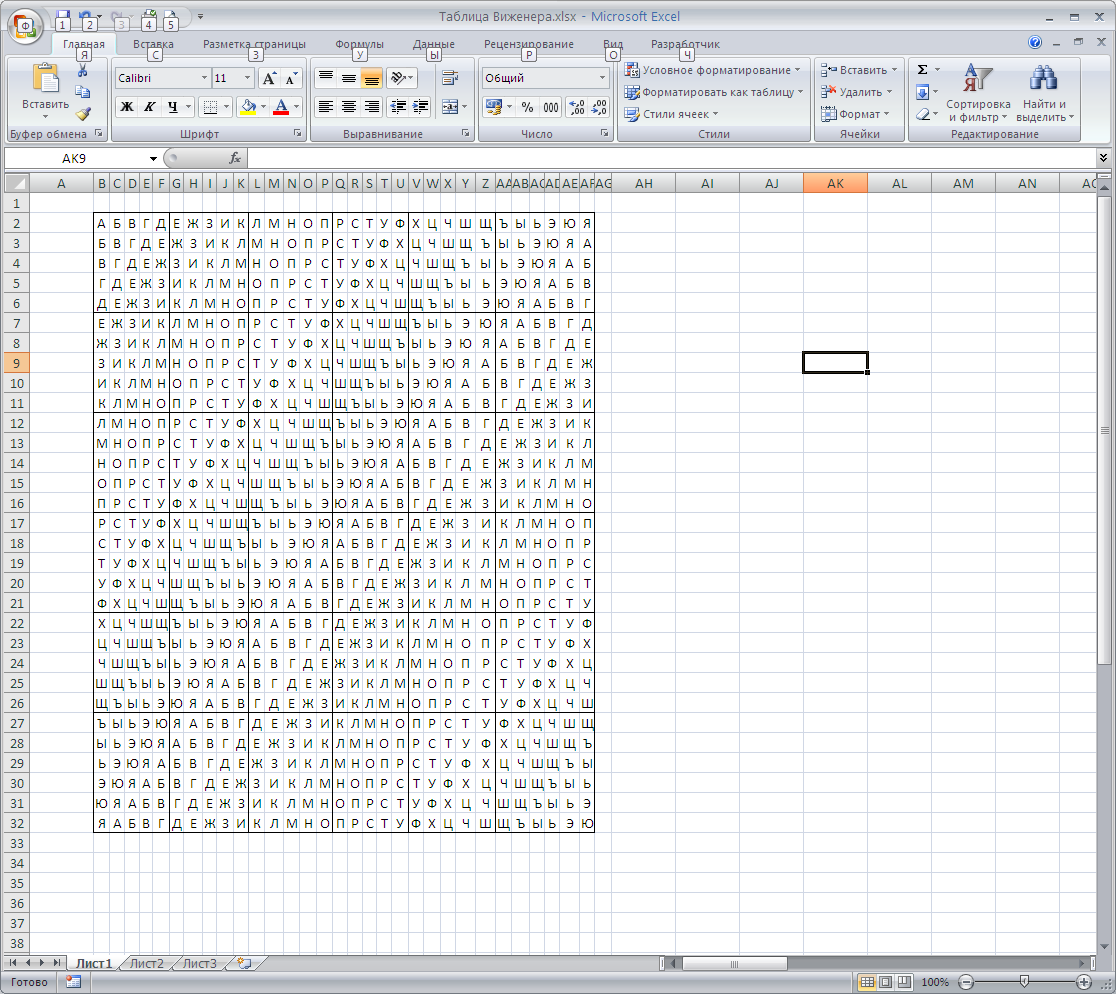


Рисунок 7 - Таблица Виженера

Далее из полной матрицы выписывают подматрицу шифрования, включающую первую строку и строки матрицы, начальными буквами которых являются последовательно буквы ключа. Наш ключ "ВЕСНА", следовательно, таблица шифрования будет следующей.

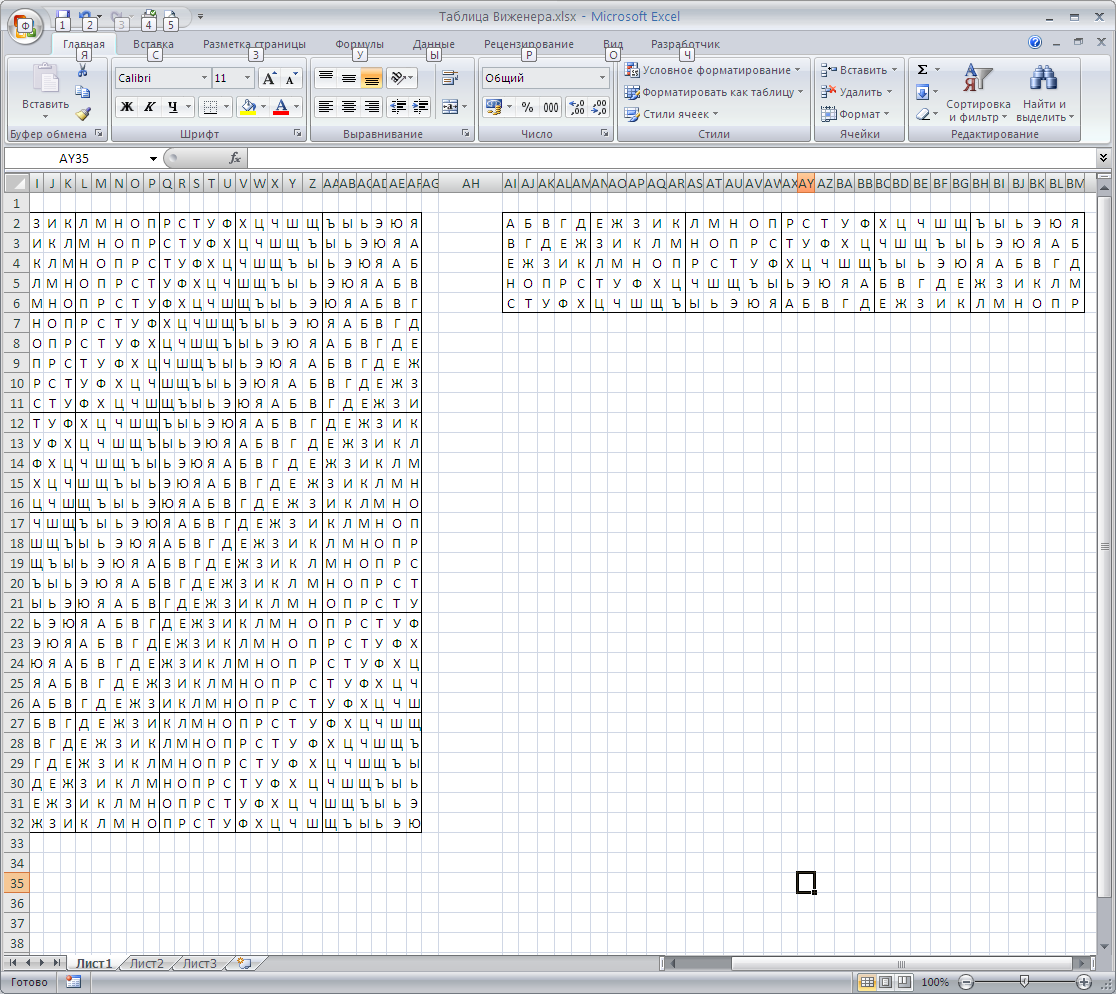


Рисунок 8 - Первый этап шифрования – составление подматрицы шифрования

В процессе шифрования () под каждой буквой шифруемого текста записывают буквы ключа, повторяющие ключ требуемое число раз, затем шифруемый текст по таблице шифрования () заменяют буквами, расположенными на пересечениях линий, соединяющих буквы текста первой строки таблицы и буквы ключа, находящейся под ней.

Например, под первой буквой исходного текста "М" записана буква "В" ключа. В таблице кодирования находим столбец, начинающийся с "М" и строку, начинающуюся с "В". На их пересечении располагается буква "О". Она и будет первым символом зашифрованного сообщения (на эта буква выделена прямоугольной рамочкой). Следующая буква исходного сообщения – "Е", символ ключа – тоже "Е". Находим пересечение строки, начинающейся с "Е", и столбца, начинающегося с "Е". Это будет буква "Л" – второй символ зашифрованного сообщения.

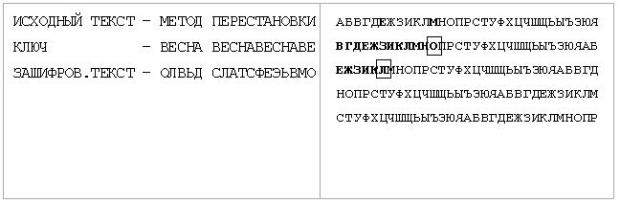


Рисунок 9 - Механизм шифрования многоалфавитной заменой

Итак, зашифрованный текст: **ОЛВЬД СЛАТСФЕЭЬВМО**.

**Задание 4.** Расшифруйте сообщение КЕКХТВОЭЦОТССВИЛ (пробелы при шифровании пропущены), зашифрованное шифром Виженера с использованием ключа ВЕСНА.

***Методические рекомендации***

Расшифровка текста выполняется в следующей последовательности ():

1. Над буквами шифрованного текста сверху последовательно записывают буквы ключа, повторяя ключ требуемое число раз.

2. В строке подматрицы таблицы Вижинера для каждой буквы ключа отыскивается буква, соответствующая знаку шифрованного текста. Находящаяся над ней буква первой строки и будет знаком расшифрованного текста.

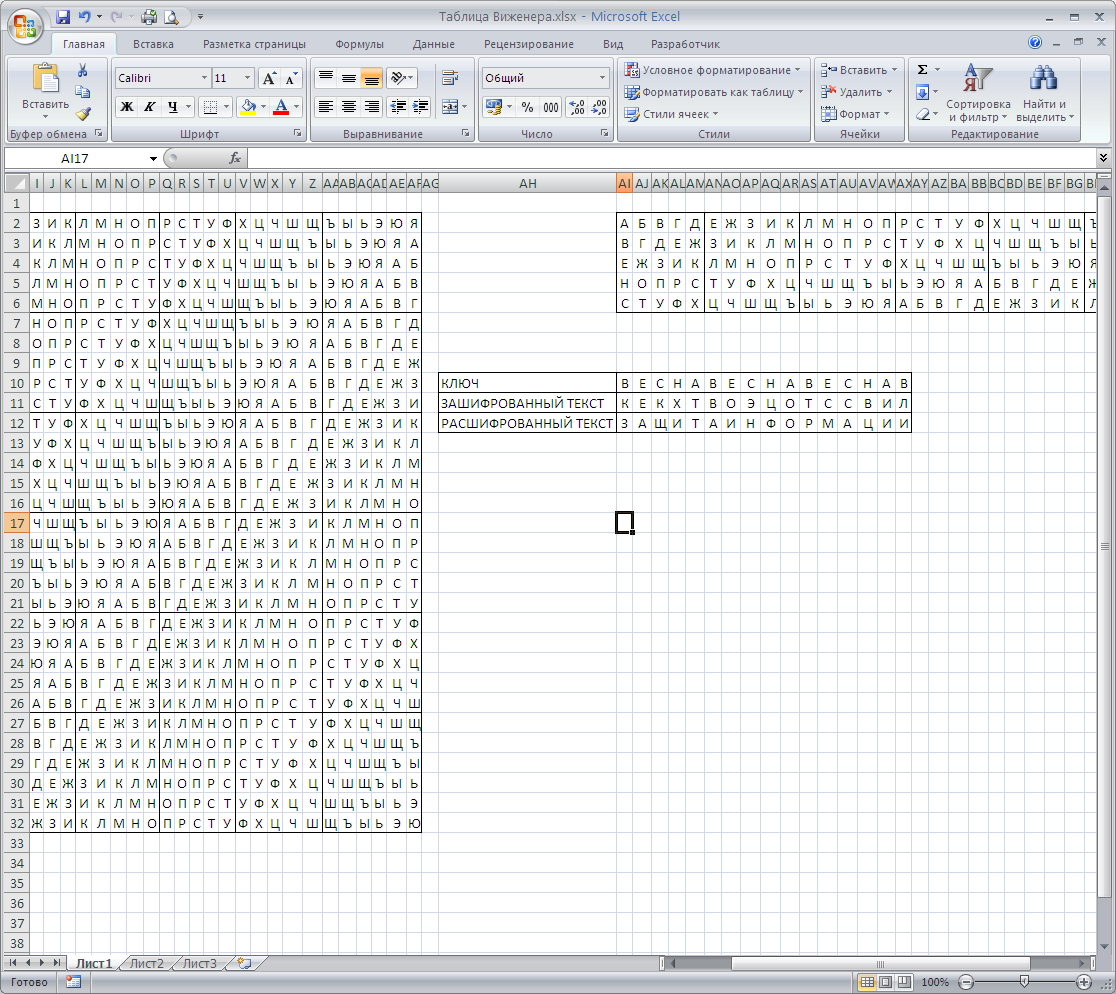


Рисунок 10 - Механизм расшифрования

3. Полученный текст группируется в слова по смыслу.

Исходный текст: ЗАЩИТА ИНФОРМАЦИИ

**Задание 5.** Зашифровать десятичное число 14 методом гаммирования с использованием ключа 12.

***Методические рекомендации***

Расшифровка текста выполняется в следующей последовательности:

1. Преобразуем исходное число и ключ (гамму) в двоичную форму:

14(10)=1110(2), 12(10)=1100(2).

2. Запишем полученные двоичные числа друг под другом и каждую пару символов сложим по модулю два. При сложении двух двоичных знаков получается 0, если исходные двоичные цифры одинаковы, и 1, если цифры разные:

Исходное число 1 1 1 0

Гамма 1 1 0 0

Результат 0 0 1 0

В результате сложения получили двоичное число 0010.

3. Переведем его в десятичную форму, получим 2.

Проверка:

Зашифрованное число 0 0 1 0

Гамма 1 1 0 0

Результат 1 1 1 0

Т.е. расшифрование производится аналогичным образом с помощью операции «сложение по модулю два».

Таким образом, в результате применения к числу 14 операции гаммирования с ключом 12 получаем в результате число 2.

**Задание 6.** Зашифровать русский текст ГАММИРОВАНИЕ методом гаммирования с использованием ключа ВЕСНА.

***Методические рекомендации***

Символы кодируются в соответствии с принятой кодировкой, а затем производится сложение по модулю 2. Если гамма короче, чем сообщение, предназначенное для зашифрования, гамма повторяется требуемое число раз. Так в примере на длина исходного сообщения равна двенадцати байтам, а длина ключа – пяти байтам. Следовательно, для зашифрования гамма должна быть повторена 2 раза полностью и еще один раз частично.



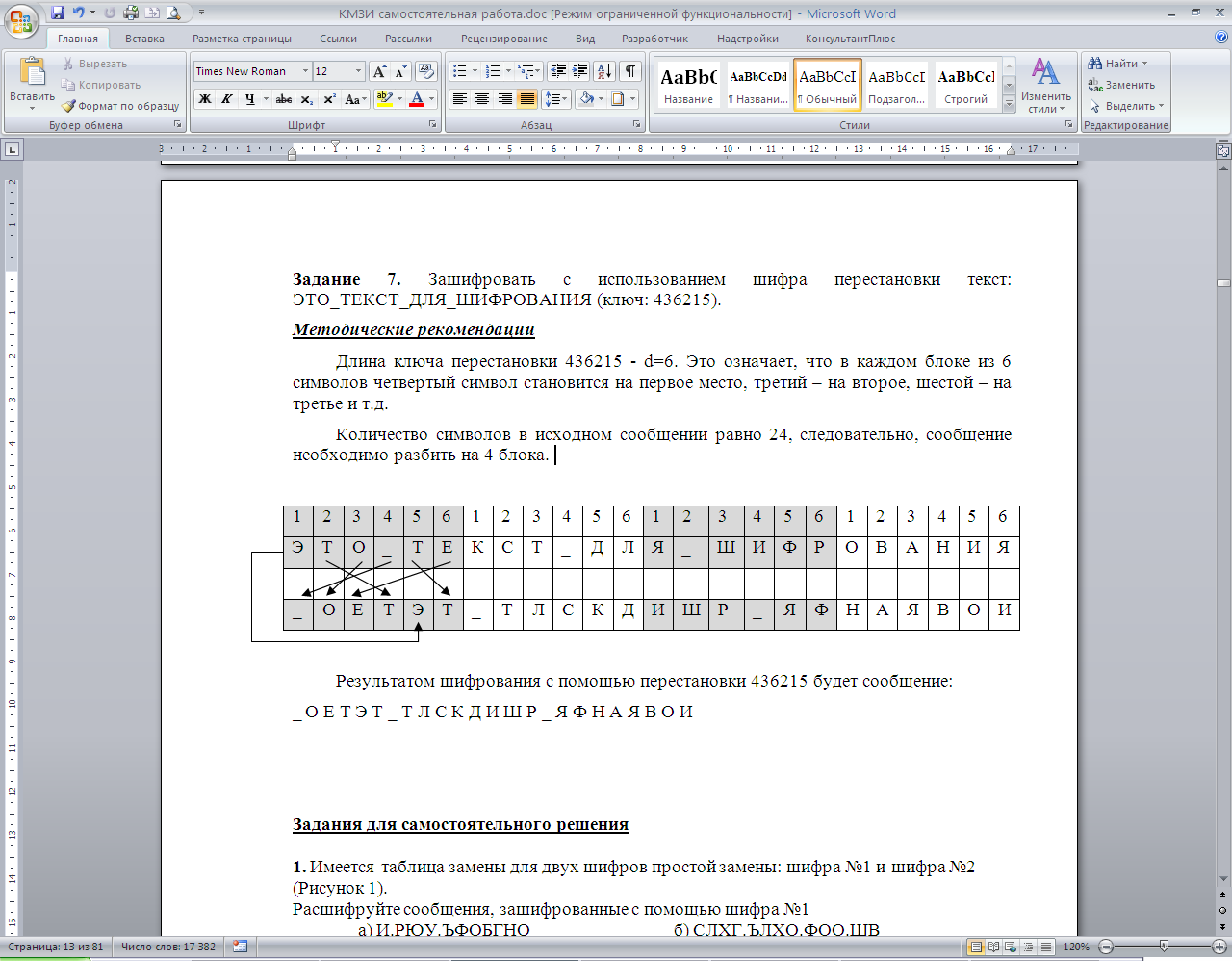
Рисунок 11 - Механизм гаммирования

**Задание 7.** Зашифровать с использованием шифра перестановки текст: ЭТО\_ТЕКСТ\_ДЛЯ\_ШИФРОВАНИЯ (ключ: 436215).

***Методические рекомендации***

Длина ключа перестановки 436215 - d=6. Это означает, что в каждом блоке из 6 символов четвертый символ становится на первое место, третий – на второе, шестой – на третье и т.д.

Количество символов в исходном сообщении равно 24, следовательно, сообщение необходимо разбить на 4 блока.



Результатом шифрования с помощью перестановки 436215 будет сообщение:

\_ О Е Т Э Т \_ Т Л С К Д И Ш Р \_ Я Ф Н А Я В О И

**Задание 8.** Зашифровать с использованием табличной перестановки текст: ЭТО\_ТЕКСТ\_ДЛЯ\_ШИФРОВАНИЯ (ключ: 3214).

***Методические рекомендации***

Ключ 3214 означает, что считывать столбцы надо так: третий, второй, первый, четвертый. Соответственно, таблица шифрования имеет 4 столбца.

Запишем текст в таблицу:

|  |  |  |  |
| --- | --- | --- | --- |
| Э | Т | О | - |
| Т | Е | К | С |
| Т | - | Д | Л |
| Я | - | Ш | И |
| Ф | Р | О | В |
| А | Н | И | Я |

Запишем столбцы в порядке 3214: ОКДШОИТЕ\_ \_РНЭТТЯФА\_СЛИВЯ.

У метода табличных перестановок могут быть различные варианты. Можно просто записывать в таблицу построчно, а считывать по столбцам в порядке следования. Можно в качестве дополнительного ключа использовать определенный размер таблицы, например, 3х4 – тогда считывание шифртекста производится в порядке 3214 сначала по первой таблице, потом по второй, т.е. результат был бы: ОКДТЕ\_ЭТТ\_СЛШОИ\_РНЯФАИВЯ.

**Задание 9.** Расшифровать с использованием табличной перестановки (таблица 3х4) текст: ПМАЕЕРНЕК.

***Методические рекомендации***

В случае, если размер сообщения не кратен размеру блока, можно дополнить сообщение какими-либо символами, не влияющими на смысл, например, пробелами. Однако это делать не рекомендуется, так как это дает противнику в случае перехвата криптограммы информацию о размере используемой таблицы перестановок (длине блока).

Шифрование сообщения, имеющего длину, не кратную размеру таблицы перестановки, например, 9 производят так: записывают сообщение в таблицу по строкам, а последние три ячейки оставим пустыми и считывают из таблицы последовательно по столбцам.

Для расшифрования вначале определяют число полных столбцов, то есть количество символов в последней строке.

Для этого делят размер сообщения (в нашем примере – 9) на количество столбцов или размер ключа (в примере – 4). Остаток от деления будет числом полных столбцов: 9 mod 4 = 1.

Следовательно, в нашем примере был 1 полный столбец и три коротких. Теперь можно поставить буквы сообщения на свои места и расшифровать сообщение.

Так как ключом при шифровании было число 1234 (столбцы считывались последовательно), то при расшифровании первые три символа (ПМА) записываются в первый столбец таблицы перестановки, следующие два (ЕЕ) – во второй столбец, следующие два (РН) – в третий, и последние два (ЕК) – в четвертый.

|  |  |  |  |
| --- | --- | --- | --- |
| П | Е | Р | Е |
| М | Е | Н | К |
| А |  |  |  |

После заполнения таблицы считываем строки и получаем исходное сообщение ПЕРЕМЕНКА.

**Задания для самостоятельного решения**

**1.** Расшифруйте сообщения, зашифрованные с помощью шифра №1 по таблице замен ().

а) И.РЮУ.ЪФОБГНО б) CЛХГ.ЪЛХО.ФОО.ЩВ

**2.** Расшифруйте сообщения, зашифрованные с помощью шифра №2:

а)  б) 

**3.** Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО сообщения:

а) КРИПТОСТОЙКОСТЬ б) ГАММИРОВАНИЕ

Исходный алфавит содержит следующие символы:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

**4.** Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа ОРЕХ:

а) ШВМБУЖНЯ б) ЯБХЪШЮМХ

Исходный алфавит состоит из следующих знаков (символ "\_" (подчеркивание) будем использовать для пробела):

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ\_

**5.** Первый байт фрагмента текста в шестнадцатеричном виде имеет вид А5. На него накладывается по модулю два 4-х битовая гамма 0111 (в двоичном виде). Что получится после шифрования?

**6.** Первый байт фрагмента текста, зашифрованного методом гаммирования (по модулю 2), в шестнадцатеричном виде имеет вид 9А. До шифрования текст имел первый байт, равный 74 (в шестнадцатеричном виде). Какой ключ использовался при шифровании?

**7.** Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщения:

а) ЖЕЛТЫЙ\_ОГОНЬ б) МЫ\_НАСТУПАЕМ

**8.** Расшифруйте сообщения, зашифрованные методом перестановки с фиксированным периодом d=8 с ключом 64275813:

а) СЛПИЬНАЕ б) РОИАГДВН

**9.** Определите ключи в системе шифрования, использующей перестановку с фиксированным периодом d=5 по парам открытых и зашифрованных сообщений:

а) МОЙ ПАРОЛЬ – ЙПМ ООЬАЛР б) СИГНАЛ БОЯ – НИСАГО ЛЯБ

**10.** Зашифруйте сообщения методом перестановки по таблице 5\*5. Ключ указывает порядок считывания столбцов при шифровании.

а) ШИРОКОПОЛОСНЫЙ УСИЛИТЕЛЬ (ключ: 41235)

б) ПЕРЕДАЧА ИЗОБРАЖЕНИЯ (ключ: 24513)

**11.** Расшифруйте сообщения, зашифрованные методом перестановки по таблице 4\*4 (символ подчеркивания заменяет пробел). Ключ указывает порядок считывания столбцов при шифровании.

а) ЕАУПД\_КЕАЗАРЧВ (ключ: 4123) б) А\_НСЫИЛБСАЛЙГ (ключ: 3142)

**12.** Известно, что при использовании шифра пропорциональной замены каждой русской букве поставлено в соответствие одно или несколько трехзначных чисел по таблице замен ().

Расшифруйте указанные сообщения.

а) 353214764134136759136762849754128212350354035767106216753211

б) 351 761756130532128759353134758105757213101752352763211762

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА:**

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных
2. Спирина М.С.,Спирин П.А.Дискретная математика:учебник: Рекомендовано ГОУВПО «МГТУ им. Н. Э. Баумана». — 9-e изд., испр. — 368 c., пер. No 7 бц.

**Интернет-ресурсы:**

www.intuit.ru

**Порядок представления материала:** на бумажном носителе или на сайте преподавателя.

**Срок представления материала:** семинарское занятие по теме.

**Форма контроля со стороны преподавателя:** собеседование

Критерии оценки: оценка «зачтено» ставится, если задачи решены правильно.

**ЛИСТ САМООЦЕНКИ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Уровень освоения | Задание 1 | Задание 2 | Задание 3 | Задание 4 | Задание 5 | Задание 6 |
| Могу помочь другим |  |  |  |  |  |  |
| Выполнил без затруднений |  |  |  |  |  |  |
| Испытывал затруднения |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Уровень освоения | Задание 7 | Задание 8 | Задание 9 | Задание 10 | Задание 11 | Задание 12 |
| Могу помочь другим |  |  |  |  |  |  |
| Выполнил без затруднений |  |  |  |  |  |  |
| Испытывал затруднения |  |  |  |  |  |  |

# Тема: «Принципы построения блочных шифров с закрытым ключом»

**Задание 1.** Сложите по модулю 2 два 16-разрядных числа: 1010 1010 1010 1010 и 0111 0011 0011 0011.

***Методические рекомендации***

Операция побитового сложения по модулю 2 обозначается XOR или \oplus. При сложении по модулю 2 операнды обрабатываются поразрядно. В разряде результата ставится единица, если в соответствующих разрядах операндов присутствует нечетное число единиц ().

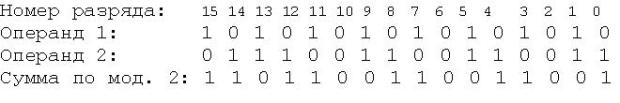


Рисунок 12 - Выполнение операции XOR

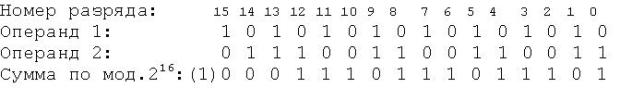
Эта операция имеет очень удобное свойство: вычитание по модулю два есть то же самое, что и сложение, поэтому один из операндов может быть получен путем прибавления к сумме другого операнда.

Ответ: 1101 1001 1001 1001.

**Задание 2.** Сложите по модулю 216 два 16-разрядных числа: 1010 1010 1010 1010 и 0111 0011 0011 0011.

***Методические рекомендации***

Также в блочных алгоритмах шифрования широко используется *операция сложения по модулю* 232 *или по модулю* 216. Эта операция представляет собой обыкновенное сложение двоичных чисел без учета переноса в старший 32-й или 16-й разряд результата.



Перенос из 15-го разряда, обозначенный в примере как единица в скобках, дальше не используется и поэтому отбрасывается.

Ответ: 0001 1101 1101 1101.

**Задание 3.** Выполните циклический сдвиг двоичного числа 1111 1111 1010 1010 влево и вправо на 3 разряда.

***Методические рекомендации***

*Циклический сдвиг* передвигает цепочку бит на некоторое число разрядов влево или вправо. Двоичное число при выполнении операции сдвига напоминает длинную гусеницу, выползающую с одной стороны туннеля и заползающую с другой. При циклическом сдвиге влево биты, выходящие слева за разрядную сетку, дописываются справа на освободившиеся места. При циклическом сдвиге вправо все биты передвигаются цепочкой вправо, а те, которым не хватает места, переносятся в хвост цепочки.

Для выполнения циклического сдвига двоичного числа влево на 3 разряда будем 3 раза переписывать двоичные цифры, каждый раз смещая их влево на 1 разряд и перенося знаки, выходящие из пятнадцатого разряда на место нулевого ().



Рисунок 13 - Операция циклического сдвига влево

Аналогично выполняется и циклический сдвиг вправо. Например, при сдвиге вправо на 3 разряда нулевой, первый и второй биты исходного числа выходят из разрядной сетки и запоминаются, все остальные биты перемещаются вправо на 3 позиции, затем запомненные цифры записываются на тринадцатое, четырнадцатое и пятнадцатое места ().



Рисунок 14 - Операция циклического сдвига вправо

|  |  |  |
| --- | --- | --- |
| **Задание 4.** Зашифруйте сообщение 1111 1111 1010 с использованием табличной подстановки.  ***Методические рекомендации***  При выполнении *табличной подстановки* группа битов отображается в другую группу битов. При этой операции один блок двоичных данных заменяется по определенному правилу или таблице другим блоком. Разобьем заданное сообщение на блоки по 3 знака: 111  111  111 010.  Заменим каждую группу из трех двоичных цифр другой группой из трех цифр по заранее определенной таблице: 000 000 000 100.  Ответ: 0000 0000 0100 | **Вход** | **Выход** |
| 000 | 110 |
| 001 | 111 |
| 010 | 100 |
| 011 | 101 |
| 100 | 010 |
| 101 | 011 |
| 110 | 001 |
| 111 | 000 |

**Задания для самостоятельного решения**

**1.** Сложите по модулю 2:

а) двоичные числа 10101100 и 11001010 ;

б) десятичные числа 15 и 10 ;

в) шестнадцатеричные числа 0В5 и 37.

Примечание: десятичные и шестнадцатеричные числа необходимо сначала перевести в двоичный вид.

**2.** Сложите по модулю 28:

а) двоичные числа 10101100 и 11001010 ;

б) десятичные числа 155 и 100 ;

в) шестнадцатеричные числа 0В5 и 37.

Примечание: десятичные числа необходимо сначала перевести в двоичный вид.

**3.** Выполните операцию циклического сдвига:

а) влево на 5 разрядов для двоичного числа 10101100 ;

б) вправо на 4 разряда для шестнадцатеричного числа 9E ;

в) вправо на 2 разряда для шестнадцатеричного числа 55.

Примечание: шестнадцатеричные числа необходимо сначала перевести в двоичный вид.

|  |  |
| --- | --- |
| **4.** Пусть каждые три бита входного сообщения заменяются по следующей таблице замен:  Выполните разбиение исходного сообщения на блоки по три бита и произведите поблочную замену для следующих сообщений, представленных в цифровом виде:  а) 1010 1100 1100(2)  б) 2356(10)  в) 0В57(16) |  |

Примечание: десятичные и шестнадцатеричные числа необходимо сначала перевести в двоичный вид.

**5.** Определите таблицу замен, используемую противником, если известно, что противник использует следующий блочный код: при шифровании каждые четыре бита входного сообщения заменяются другими четырьмя битами по определенной таблице замен. Удалось перехватить одну пару сообщений "исходный текст" - "зашифрованный текст". Все сообщения представлены в шестнадцатеричном формате.

Исходное сообщение: 5A 43 63 19 1E D0 C7 4B F0 8A

Зашифрованное сообщение: 92 37 A7 C0 CE 6B F1 35 8B D2

**6.** Определите таблицы замен, используемые противником, если известно, что после вскрытия блочного шифра, описанного в задании 5, коварный противник решил усложнить используемую схему шифрования следующим образом: при шифровании сообщение разбивается на блоки по восемь бит; первые четыре бита входного сообщения заменяются другими четырьмя битами по одной таблице замен, а вторые четыре бита – по другой таблице замен. Удалось перехватить две пары сообщений **"исходный текст" - "зашифрованный текст"**. Все сообщения представлены в шестнадцатеричном формате.

а) Исходное сообщение 1: 5A 4D 6B 19 1E 3F 7C 47 F8

Зашифрованное сообщение 1: 98 35 AC C1 CE 79 12 34 8D

б) Исходное сообщение 2: A3 D0 84 F1 96 C8 E5 77 2B

Зашифрованное сообщение 2: 2B 66 D0 8A 0F FD E7 14 4C

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА:**

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных
2. Спирина М.С.,Спирин П.А.Дискретная математика:учебник: Рекомендовано ГОУВПО «МГТУ им. Н. Э. Баумана». — 9-e изд., испр. — 368 c., пер. No 7 бц.

**Интернет-ресурсы:**

www.intuit.ru

**Порядок представления материала:** на бумажном носителе или на сайте преподавателя.

**Срок представления материала:** семинарское занятие по теме.

**Форма контроля со стороны преподавателя:** собеседование

Критерии оценки: оценка «зачтено» ставится, если задачи решены правильно.

**ЛИСТ САМООЦЕНКИ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Уровень освоения | Задание 1 | Задание 2 | Задание 3 | Задание 4 | Задание 5 | Задание 6 |
| Могу помочь другим |  |  |  |  |  |  |
| Выполнил без затруднений |  |  |  |  |  |  |
| Испытывал затруднения |  |  |  |  |  |  |

# Тема: «Криптографические хеш-функции»

**Задание 1.** Найдите значение хеш-функции для исходного сообщения 3E 54 A0 1F B4, если известно, что хеш-функция образуется следующим образом: складываем все байты входной строки по модулю 2 и байт-результат возвращаем в качестве значения хеш-фукнции.

***Методические рекомендации***

Под термином хеш-функция понимается функция, отображающая электронные сообщения произвольной длины в значения фиксированной длины. Т.о. у всякой хеш-функции *h* имеется большое количество коллизий, т.е. пар значений х и у таких, что *h(x)=h(y)*. Основное требование, предъявляемое криптографическими приложениями к хеш-функциям, состоит в отсутствии эффективных алгоритмов поиска коллизий. Кроме того, хеш-функция должна быть односторонней, т.е. функцией, по значению которой вычислительно трудно найти её аргумент, в то же время, функцией, для аргумента которой вычислительно трудно найти другой аргумент, который давал бы то же самое значение функции. Схемы электронной цифровой подписи – основная сфера применения хеш-функций.

Простейшая хеш-функция может быть составлена с использованием операции "сумма по модулю 2" следующим образом: получаем входную строку, складываем все байты по модулю 2 и байт-результат возвращаем в качестве значения хеш-фукнции. Длина значения хеш-функции составит в этом случае 8 бит независимо от размера входного сообщения.

Переведем исходное сообщение 3E 54 A0 1F B4 в двоичный вид, запишем байты друг под другом и сложим биты в каждом столбике по модулю 2:

|  |
| --- |
| 0011 1110 |
| 0101 0100 |
| 1010 0000 |
| 0001 1111 |
| 1011 0100 |
| 0110 0101 |

Результат 0110 0101(2) или 65(16) ) и будет значением хеш-функции.

**Задание 2.** Найдите значение хеш-функции для сообщения «ДВА» при помощи хеш-функции с параметрами *p*=7, *q*=3, вектор инициализации *I*=6 (выбираем случайно), если известно, что хеш-функция образуется следующим образом: *Hi=[(Hi-1⊕Mi)2] (mod n)*, где *i=1…n*; *H0=0*; *M=M1, M2, …, Mn*. Длина блока *Mi* представляется в октетах, каждый октет разбит пополам и к каждой половине спереди приписывается полуоктет, состоящий из двоичных единиц: *n* – произведение двух больших (512-битных) простых чисел *p* и *q*..

***Методические рекомендации***

Один из практических методов построения хеш-функций - на основе какой-либо известной вычислительно трудной математической задачи. Например, легко вычислить квадрат числа по модулю *n: х2 (mod n)*, но вычислительно трудно извлечь квадратный корень по этому модулю. Т.о., хеш-функцию можно записать так: *Hi=[(Hi-1⊕Mi)2] (mod n)*, где *i=1…n*; *H0=0*; *M=M1, M2, … , Mn*. Длина блока *Mi* представляется в октетах, каждый октет разбит пополам и к каждой половине спереди приписывается полуоктет, состоящий из двоичных единиц: *n* – произведение двух больших (512-битных) простых чисел *p* и *q*.

Итак, для решения нашей задачи будем придерживаться следующего алгоритма:

1). Получаем значение модуля: n=pq=7⋅3=21;

2). Представим сообщение «ДВА» в числовом эквиваленте (по номеру буквы в алфавите):

ДВА→5 3 1

3). Представим коды битовой строкой:

5 3 1

00000101 00000011 00000001

*I*=610=000001102.

4). Разбиваем байт пополам (разбиение октета на полуоктеты), добавляем в начало полубайта единицы и получаем хешируемые блоки *Mi*:

*М1 М2  М3 М4 М5 М6*

11110000 11110101 11110000 11110011 11110000 11110001.

5). Выполняем итеративные шаги:

Первая итерация:

М1=11110000,

Н0= 00000110,

Н0⊕М1= 111101102=24610,

[(Н0⊕М1)]2(mod 21)=2462(mod 21)=152(mod 21)=(-6)2(mod 21)=15,

H1=1510=0000111112.

Вторая итерация:

М2=11110101,

Н1= 00001111,

Н1⊕М2= 111110102=25010,

[(Н1⊕М2)]2 (mod 21)=2502 (mod 21)= 192(mod 21)=(-2)2(mod 21)=4,

H2=410=000001002.

И т.д. Всего нужно выполнить шесть итераций, полученное число Н6 и будет хеш-код.

**Задания для самостоятельного решения**

**1.** Для каждого из шести сообщений, записанных в левом столбце, найдите соответствующий результат вычисления хеш-функции из правого столбца. Хеш-функция y=h(x1x2…xn) определяется как результат выполнения побитовой операции "сумма по модулю 2" для всех байтов сообщения, представленного в двоичном виде. Длина хеш-кода равна 8 битам. Все сообщения и значения хеш-функции представлены в шестнадцатеричном формате.

|  |  |
| --- | --- |
| **Сообщения** | **Значения хеш-функции** |
| 0A3 69 2C | 38 |
| 82 0F B5 | 1B |
| 0DA 14 90 | 0F9 |
| 32 01 BF | 8C |
| 9E A6 23 | 0E6 |
| 10 ВE 57 | 5E |

**2.** Получить хеш-код для сообщения «HASHING» при помощи хеш-функции, описанной в Задаче 2 с параметрами p=17, q=19, кодируя буквы:

* 1. порядковым номером в алфавите;
  2. ASCII – символами (HASHING: 72-65-83-72-73-78-71).

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА:**

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных
2. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования
3. Спирина М.С.,Спирин П.А.Дискретная математика:учебник: Рекомендовано ГОУВПО «МГТУ им. Н. Э. Баумана». — 9-e изд., испр. — 368 c., пер. No 7 бц.

**Интернет-ресурсы:**

www.intuit.ru

**Порядок представления материала:** на бумажном носителе или на сайте преподавателя.

**Срок представления материала:** семинарское занятие по теме.

**Форма контроля со стороны преподавателя:** собеседование

Критерии оценки: оценка «зачтено» ставится, если задачи решены правильно.

**ЛИСТ САМООЦЕНКИ**

|  |  |  |
| --- | --- | --- |
| Уровень освоения | Задание 1 | Задание 2 |
| Могу помочь другим |  |  |
| Выполнил без затруднений |  |  |
| Испытывал затруднения |  |  |

# Тема: «Поточные шифры и генераторы псевдослучайных чисел»

**Задание 1.** Определите первые восемь чисел и период линейного конгруэнтного генератора ПСЧ для параметров a=5, b=3, c=11 и пусть k0= 1.

***Методические рекомендации***

Генераторы псевдослучайных чисел могут работать по разным алгоритмам. Одним из простейших генераторов является так называемый **линейный конгруэнтный генератор**, который для вычисления очередного числа ki использует формулу

ki=(a\*ki-1+b) mod c,

где а, b, с — некоторые константы, a ki-1 — предыдущее псевдослучайное число. Для получения k1 задается начальное значение k0.

В данном примере a=5,b=3,c=11 и пусть k0= 1. В этом случае мы будем использовать формулу ki=(5\*ki-1+3) mod 11. Вычислим несколько элементов последовательности:

k1 = (5 \* 1 + 3) mod 11 = 8;

k2 = (5 \* 8 + 3) mod 11 = 10;

k3 = (5 \* 10 + 3) mod 11 = 9;

k4 = (5 \* 9 + 3) mod 11 = 4;

k5 = (5 \* 4 + 3) mod 11 = 1;

k6 = (5 \* 1 + 3) mod 11 = 8,

k7 = (5 \* 8 + 3) mod 11 = 10;

k8= (5 \* 10 + 3) mod 11 = 9.

Полученные значения (8, 10, 9, 4, 1) выглядят похожими на случайные числа. Однако следующее значение k6 будет снова равно 8, а значения k7 и k8 будут равны 10 и 9 соответственно:

Выходит, наш генератор псевдослучайных чисел повторяется, порождая периодически числа 8, 10, 9, 4, 1. К сожалению, это свойство характерно для всех линейных конгруэнтных генераторов. Изменяя значения основных параметров a, b и c, можно влиять на длину периода и на сами порождаемые значения ki. Так, например, увеличение числа с в общем случае ведет к увеличению периода. Если параметры a, b и c выбраны правильно, то генератор будет порождать случайные числа с максимальным периодом, равным c. При программной реализации значение с обычно устанавливается равным 2b-1 или 2b, где b — длина слова ЭВМ в битах.

Ответ: найденные числа: 8, 10, 9, 4, 1, 8, 10, 9; период 5.

**Задание 2.** Вычислите последовательность из десяти чисел, генерируемую методом Фибоначчи с запаздыванием начиная с kа при следующих исходных данных: a = 4, b = 1, k0=0.1; k1=0.7; k2=0.3; k3=0.9; k4=0.5.

***Методические рекомендации***

Метод Фибоначчи с запаздываниями— один из методов генерации псевдослучайных чисел -позволяет получить более высокое "качество" псевдослучайных чисел.

Для вычисления последовательности случайных чисел по методу Фибоначчи используется рекуррентная формула:

где ki — вещественные числа из диапазона [0,1], a, b — целые положительные числа, параметры генератора.

Вычислим последовательность из первых десяти чисел, генерируемую методом Фибоначчи с запаздыванием начиная с k5 при следующих исходных данных: a = 4, b = 1, k0=0.1; k1=0.7; k2=0.3; k3=0.9; k4=0.5:

k5 = k1 - k4 = 0.7 - 0.5 = 0.2;

k6 = k2 - k5= 0.3 - 0.2 = 0.1;

k7 = k3 - k6 = 0.9 - 0.1 = 0.8;

k8 = k4 - k7 + 1 =0.5 - 0.8 + 1 = 0.7;

k9 = k5- k8 + 1 =0.2 - 0.7 + 1 = 0.5;

k10 = k6 - k9 + 1 =0.1 - 0.5 + 1 = 0.6;

k11 = k7 - k10 = 0.8 - 0.6 = 0.2;

k12 = k8 - k11 = 0.7 - 0.2 = 0.5;

k13 = k9 - k12 + 1 =0.5 - 0.5 + 1 = 1;

k14 = k10 - k13 + 1 =0.6 - 1 + 1 = 0.6.

Видим, что генерируемая последовательность чисел внешне похожа на случайную. И действительно, исследования подтверждают, что получаемые случайные числа обладают хорошими статистическими свойствами.

Для генераторов, построенных по методу Фибоначчи с запаздыванием, существуют рекомендуемые параметры a и b, так сказать, протестированные на качество. Например, исследователи предлагают следующие значения: (a,b) = (55, 24), (17, 5) или (97,33).

Ответ: найденные числа: 0.2, 0.1, 0.8, 0.7, 0.5, 0.6, 0.2, 0.5, 1, 0.6.

**Задание 3.** Вычислить первые десять чисел по методу генерации псевдослучайных чисел BBS, если p = 11, q = 19, х = 3.

***Методические рекомендации***

Алгоритм BBS (от фамилий авторов — L. Blum, M. Blum, M. Shub) или генератор с квадратичным остатком также предназначен для генерации псевдослучайных чисел.

Он заключается в следующем. Вначале выбираются два больших простых числа p и q. Числа p и q должны быть оба *сравнимы* с 3 по модулю 4, то есть при делении p и q на 4 должен получаться одинаковый остаток 3. Далее вычисляется число M = p\* q, называемое целым числом Блюма. Затем выбирается другое случайное целое число х, взаимно простое (то есть не имеющее общих делителей, кроме единицы) с М. Вычисляем х0= х2mod M. х0 называется стартовым числом генератора.

На каждом n-м шаге работы генератора вычисляется хn+1= хn2 mod M. Результатом n-го шага является один (обычно младший) бит числа хn+1. Иногда в качестве результата принимают бит чётности, то есть количество единиц в двоичном представлении элемента. Если количество единиц в записи числа четное – бит четности принимается равным 0, нечетное – бит четности принимается равным 1.

В данном примере p = 11, q = 19 (убеждаемся, что 11 mod 4 = 3, 19 mod 4 = 3). Тогда M = p\* q = 11\*19=209.

Выберем х, взаимно простое с М: пусть х = 3. Вычислим стартовое число генератора х0:

х0 = х2 mod M = 32 mod 209 = 9 mod 209 = 9.

Вычислим первые десять чисел хi по алгоритму BBS. В качестве случайных бит будем брать младший бит в двоичной записи числа хi:

|  |  |  |
| --- | --- | --- |
| х1=92 mod 209= 81 mod 209= 81 | младший бит: | 1 |
| х2=812 mod 209= 6561 mod 209= 82 | младший бит: | 0 |
| х3=822 mod 209= 6724 mod 209= 36 | младший бит: | 0 |
| х4=362 mod 209= 1296 mod 209= 42 | младший бит: | 0 |
| х5=422 mod 209= 1764 mod 209= 92 | младший бит: | 0 |
| х6=922 mod 209= 8464 mod 209= 104 | младший бит: | 0 |
| х7=1042 mod 209= 10816 mod 209= 157 | младший бит: | 1 |
| х8=1572 mod 209= 24649 mod 209= 196 | младший бит: | 0 |
| х9=1962 mod 209= 38416 mod 209= 169 | младший бит: | 1 |
| х10=1692 mod 209= 28561 mod 209= 137 | младший бит: | 1 |

Самым интересным для практических целей свойством этого метода является то, что для получения n-го числа последовательности не нужно вычислять все предыдущие n чисел хi. Оказывается хn можно сразу получить по формуле

x_n=x_0^{2^n mod ((p-1)(q-1)} mod \: M

Например, вычислим х10 сразу из х0:

x_{10}=x_0^{2^{10} mod ((11-1)(19-1)} mod \ 209 = x_0^{1024 mod \ 180} mod \ 209 =\\
9^{124} \ mod \ 209=(9^4)^{31} \ mod \ 209=81^{31} \ mod \ 209 =\\
(82^{15} \ mod \ 209)(81^{16} \ mod \ 209)=((81^3)^5) \ mod \ 209)((81^4)^4) \ mod \ 209)=\\
(26^5 \ mod \ 209)(42^4 \ mod \ 209)=(144*104) \ mod \ 209=14976 \ mod \ 209=137

В результате действительно получили такое же значение, как и при последовательном вычислении, – 137. Вычисления кажутся достаточно сложными, однако на самом деле их легко оформить в виде небольшой процедуры или программы и использовать при необходимости.

**Задания для самостоятельного решения**

**1.** Определите последовательность из первых десяти чисел и период линейного конгруэнтного генератора ПСЧ для различных параметров а, b и c (k0 принять равным 0):

а) а =5, b =7 и c = 17;

б) а = 6, b =3 и c = 23.

**2.** Значения k0, k1, k2, k3, полученные с помощью линейного конгруэнтного генератора, равны: k0 = 1, k1 = 12, k2 = 3, k3 = 6. Найдите параметры а, b и c генератора ПСЧ.

**3.** Вычислите последовательность из десяти чисел, генерируемую методом Фибоначчи с запаздыванием начиная с kа при следующих исходных данных:

а) a = 3, b = 1, k0=0.6; k1=0.3; k2=0.5;

б) a = 4, b = 2, k0=0.9; k1=0.3; k2=0.5; k3=0.9.

**4.** Вычислить х11 по методу генерации псевдослучайных чисел BBS, если p = 11, q = 19, х = 3.

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА:**

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных
2. Спирина М.С.,Спирин П.А.Дискретная математика:учебник: Рекомендовано ГОУВПО «МГТУ им. Н. Э. Баумана». — 9-e изд., испр. — 368 c., пер. No 7 бц.

**Интернет-ресурсы:**

www.intuit.ru

**Порядок представления материала:** на бумажном носителе или на сайте преподавателя.

**Срок представления материала:** семинарское занятие по теме.

**Форма контроля со стороны преподавателя:** собеседование

Критерии оценки: оценка «зачтено» ставится, если задачи решены правильно.

**ЛИСТ САМООЦЕНКИ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Уровень освоения | Задание 1 | Задание 2 | Задание 3 | Задание 4 |
| Могу помочь другим |  |  |  |  |
| Выполнил без затруднений |  |  |  |  |
| Испытывал затруднения |  |  |  |  |

# Тема: «Поточные шифры и генераторы псевдослучайных чисел»

**Задание 1.** Вычислите последовательность внутренних состояний сдвигового регистра с обратной связью, представленного на с заданным начальным значением 1011.

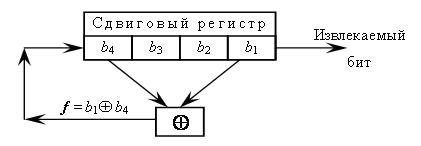


Рисунок 15 - Пример 4-разрядного линейного сдвигового регистра

***Методические рекомендации***

Запишем в изображенный на рисунке регистр начальное значение 1011. Вычислять последовательность внутренних состояний регистра удобно с помощью таблицы, представленной на таблице ниже. В таблице отражены первые девять состояний регистра.

На каждом шаге все содержимое регистра сдвигается вправо на один разряд. При этом можно получить в качестве результата один бит. На освободившееся слева место поступает бит, равный результату вычисления функции обратной связи f = b_1 \oplus b_4. Выходную последовательность генератора псевдослучайных бит образует последний столбец таблицы (извлекаемый бит).

|  |  |  |  |
| --- | --- | --- | --- |
| **Номер состояния** | **Внутреннее состояние регистра b4, b3, b2, b1** | **Результат вычисления функции обратной связи**  **f = b_1 \oplus b_4** | **Извлекаемый бит ( b1 )** |
| 0 | 1 0 1 1 | 0 | 1 |
| 1 | 0 1 0 1 | 1 | 1 |
| 2 | 1 0 1 0 | 1 | 0 |
| 3 | 1 1 0 1 | 0 | 1 |
| 4 | 0 1 1 0 | 0 | 0 |
| 5 | 0 0 1 1 | 1 | 1 |
| 6 | 1 0 0 1 | 0 | 1 |
| 7 | 0 1 0 0 | 0 | 0 |
| 8 | 0 0 1 0 | 0 | 0 |

Основным недостатком генераторов псевдослучайных чисел на базе линейных сдвиговых регистров является сложность программной реализации. Сдвиги и битовые операции легко и быстро выполняются в электронной аппаратуре, поэтому в разных странах выпускаются микросхемы и устройства для поточного шифрования на базе алгоритмов с использованием сдвиговых регистров с обратной связью.

**Задание 2.** Вычислите последовательность из десяти чисел, генерируемую методом Фибоначчи с запаздыванием начиная с kа при следующих исходных данных: a = 4, b = 1, k0=0.1; k1=0.7; k2=0.3; k3=0.9; k4=0.5.

***Методические рекомендации***

Метод Фибоначчи с запаздываниями— один из методов генерации псевдослучайных чисел -позволяет получить более высокое "качество" псевдослучайных чисел.

Для вычисления последовательности случайных чисел по методу Фибоначчи используется рекуррентная формула:

где ki — вещественные числа из диапазона [0,1], a, b — целые положительные числа, параметры генератора.

Вычислим последовательность из первых десяти чисел, генерируемую методом Фибоначчи с запаздыванием начиная с k5 при следующих исходных данных: a = 4, b = 1, k0=0.1; k1=0.7; k2=0.3; k3=0.9; k4=0.5:

k5 = k1 - k4 = 0.7 - 0.5 = 0.2;

k6 = k2 - k5= 0.3 - 0.2 = 0.1;

k7 = k3 - k6 = 0.9 - 0.1 = 0.8;

k8 = k4 - k7 + 1 =0.5 - 0.8 + 1 = 0.7;

k9 = k5- k8 + 1 =0.2 - 0.7 + 1 = 0.5;

k10 = k6 - k9 + 1 =0.1 - 0.5 + 1 = 0.6;

k11 = k7 - k10 = 0.8 - 0.6 = 0.2;

k12 = k8 - k11 = 0.7 - 0.2 = 0.5;

k13 = k9 - k12 + 1 =0.5 - 0.5 + 1 = 1;

k14 = k10 - k13 + 1 =0.6 - 1 + 1 = 0.6.

Видим, что генерируемая последовательность чисел внешне похожа на случайную. И действительно, исследования подтверждают, что получаемые случайные числа обладают хорошими статистическими свойствами.

Для генераторов, построенных по методу Фибоначчи с запаздыванием, существуют рекомендуемые параметры a и b, так сказать, протестированные на качество. Например, исследователи предлагают следующие значения: (a,b) = (55, 24), (17, 5) или (97,33).

Ответ: найденные числа: 0.2, 0.1, 0.8, 0.7, 0.5, 0.6, 0.2, 0.5, 1, 0.6.

**Задание 3.** Сгенерируйтеь последовательность пяти первых чисел по алгоритму RC4, если секретный ключ состоит из шести 4-битовых значений (приведем их в десятичном виде): 1, 2, 3, 4, 5, 6.

***Методические рекомендации***

Алгоритм **RC4** разработан Р.Ривестом специально как генератор потока ключевой информации с ключом переменной длины.

Алгоритм RC4 состоит из двух этапов. На первом, подготовительном этапе производится инициализация таблицы замен S. На втором, основном этапе вычисляются псевдослучайные числа.

|  |  |
| --- | --- |
| Посмотрим, как инициализируется таблица S. Вначале она заполняется последовательно числами от 0 до 15. Ключ представляется в виде последовательности 4-битовых слов, которыми заполняется другой массив K, такого же размера, как S. Если ключ оказался короче, чем надо, он повторяется нужное число раз. Затем выполняются следующие действия ( *алгоритм 1* ) | ***Алгоритм 1***  **1.** j = 0; i =0;  **2.** j = (j + Si + Ki) mod 16;  **3.** поменять местами Si и Sj;  **4.** i = i +1;  **5.** если i <16, то перейти на п.2 |

В результате выполнения этого алгоритма производится начальное заполнение таблицы замен S, причем это начальное перемешивание значений производится в зависимости от секретного ключа.

|  |  |
| --- | --- |
| После того, как таблица S подготовлена, можно начинать генерацию случайных n-битовых слов. Для этого счетчикам i и j присваивается начальное значение 0. Затем для получения каждого нового значения zi выполняются следующие действия (*алгоритм 2*). | ***Алгоритм 2***  **1.** i = (i + 1) mod 16;  **2.** j = (j + Si) mod 16;  **3.** поменять местами Si и Sj;  **4.** a = (Si + Sj) mod 16;  **5.** zi = Sa. |

Полученное 4-битовое значение zi может использоваться в качестве ключа для шифрования очередного 4-битового блока входного потока данных.

Например, пусть секретный ключ состоит из шести 4-битовых значений (приведем их в десятичном виде): 1, 2, 3, 4, 5, 6. Попробуем сгенерировать последовательность чисел по алгоритму RC4.

Заполним таблицу S последовательно числами от 0 до 15.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер элемента | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Значение | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

Затем подготовим таблицу K, записав в нее ключ необходимое количество раз:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер элемента | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Значение | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 |

Затем перемешаем содержимое таблицы S. Для этого будем использовать алгоритм 1, описанный выше. Процесс выполнения представим в виде трассировочной таблицы, в которой укажем все производимые действия. При выполнении вычислений необходимо помнить, что все операции сложения выполняются по модулю 16.

Подготовительный этап (инициализация таблицы замен) алгоритма RC4

|  |  |  |  |
| --- | --- | --- | --- |
| **Номер пункта алг.** | **Выполняемое действие (по mod 16)** | **Новое значение i** | **Новое значение j** |
| 1 | **j = 0; i =0** | 0 |  |
| 2 | j = j + Si + Ki = 0 + 0 + 1 = 1 |  | 1 |
| 3 | Поменять местами Si и Sj, то есть S0 и S1 |  |  |
| 4 | i = i +1 | 1 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = j + Si + Ki = 1 + 0+ 2 = 3 |  | 3 |
| 3 | Поменять местами Si и Sj, то есть S1 и S3 |  |  |
| 4 | i = i +1 | 2 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (3 + 2 + 3) mod 16 = 8 |  | 8 |
| 3 | Поменять местами Si и Sj , то есть S2 и S8 |  |  |
| 4 | i = i +1 | 3 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (8 + 0 + 4) mod 16 = 12 |  | 12 |
| 3 | Поменять местами Si и Sj , то есть S3 и S12 |  |  |
| 4 | i = i +1 | 4 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (12 + 4 + 5) mod 16 = 5 |  | 5 |
| 3 | Поменять местами Si и Sj , то есть S4 и S5 |  |  |
| 4 | i = i +1 | 5 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (5 + 4 + 6) mod 16 = 15 |  | 15 |
| 3 | Поменять местами Si и Sj , то есть S5 и S15 |  |  |
| 4 | i = i +1 | 6 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (15 + 6 + 1) mod 16 = 6 |  | 6 |
| 3 | Поменять местами Si и Sj , то есть S6 и S6 |  |  |
| 4 | i = i +1 | 7 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (6 + 7 + 2) mod 16 = 15 |  | 15 |
| 3 | Поменять местами Si и Sj , то есть S7 и S15 |  |  |
| 4 | i = i +1 | 8 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (15 + 2 + 3) mod 16 = 4 |  | 4 |
| 3 | Поменять местами Si и Sj , то есть S8 и S4 |  |  |
| 4 | i = i +1 | 9 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (4 + 9 + 4) mod 16 = 1 |  | 1 |
| 3 | Поменять местами Si и Sj , то есть S9 и S1 |  |  |
| 4 | i = i +1 | 10 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (1 + 10 + 5) mod 16 = 0 |  | 0 |
| 3 | Поменять местами Si и Sj , то есть S10 и S0 |  |  |
| 4 | i = i +1 | 11 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (0 + 11 + 6) mod 16 = 1 |  | 1 |
| 3 | Поменять местами Si и Sj , то есть S11 и S1 |  |  |
| 4 | i = i +1 | 12 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (1 + 0 + 1) mod 16 = 2 |  | 2 |
| 3 | Поменять местами Si и Sj , то есть S12 и S2 |  |  |
| 4 | i = i +1 | 13 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (2 + 13 + 2) mod 16 = 1 |  | 1 |
| 3 | Поменять местами Si и Sj , то есть S13 и S1 |  |  |
| 4 | i = i +1 | 14 |  |
| 5 | i < 16, поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (1 + 14 + 3) mod 16 = 2 |  | 2 |
| 3 | Поменять местами Si и Sj , то есть S14 и S2 |  |  |
| 4 | i = i +1 | 15 |  |
| 5 | i < 16 , поэтому перейти на п.2 |  |  |
| 2 | j = (j + Si + Ki ) mod 16= (2 + 7 + 4) mod 16 = 13 |  | 13 |
| 3 | Поменять местами Si и Sj , то есть S15 и S13 |  |  |
| 4 | i = i +1 | 16 |  |
| 5 | i < 16 – неверно, поэтому закончить |  |  |

После выполнения алгоритма 1 получим инициализированную и подготовленную к основному этапу таблицу S:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер элемента | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Значение | 10 | 13 | 14 | 12 | 2 | 15 | 6 | 4 | 5 | 3 | 1 | 9 | 8 | 7 | 0 | 11 |

После того как таблица S подготовлена, можно начинать генерацию случайных 4-битовых слов. Вычислим первые 5 чисел псевдослучайной последовательности, используя алгоритм 2. Результаты вычисления последовательности значений также представим в виде таблицы.

Основной этап (вычисление элементов псевдослучайной последовательности) алгоритма RC4:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Выполняемое действие (по mod 16)** | **Новое знач. i** | **Новое знач. j** | **Новое знач. а** |
| Вычисление z1 | 1. i = (i + 1) =0+1=1 | 1 |  |  |
| 2. j = (j + Si) mod 16=(0+13) mod 16=13 |  | 13 |  |
| 3. Поменять местами S1 и S13 |  |  |  |
| 4. a = (Si + Sj )mod 16=(7+13)mod 16=4 |  |  | 4 |
| 5. z1 = S4 =2 |  |  |  |
| Вычисление z2 | 1. i = (i + 1) =1+1=2 | 2 |  |  |
| 2. j = (j + Si) mod 16=(13+14) mod 16=11 |  | 11 |  |
| 3. Поменять местами S2 и S11 |  |  |  |
| 4. a = (Si + Sj )mod 16=(9+14)mod 16=7 |  |  | 7 |
| 5. z2 = S7=4 |  |  |  |
| Вычисление z3 | 1. i = (i + 1) =2+1=3 | 3 |  |  |
| 2. j = (j + Si) mod 16=(11+12) mod 16=7 |  | 7 |  |
| 3. Поменять местами S3 и S7 |  |  |  |
| 4. a = (Si + Sj )mod 16=(4+12)mod 16=0 |  |  | 0 |
| 5. z3 = S0=10 |  |  |  |
| Вычисление z4 | 1. i = (i + 1) =3+1=4 | 4 |  |  |
| 2. j = (j + Si) mod 16=(7+2) mod 16=9 |  | 9 |  |
| 3. Поменять местами S4 и S9 |  |  |  |
| 4. a = (Si+ Sj ) mod 16=(3+2)mod 16=5 |  |  | 5 |
| 5. z4= S5=15 |  |  |  |
| Вычисление z5 | 1. i = (i + 1) =4+1=5 | 5 |  |  |
| 2. j = (j + Si) mod 16=(9+15) mod 16=8 |  | 8 |  |
| 3. Поменять местами S5 и S8 |  |  |  |
| 4. a = (Si+ Sj)mod 16=(5+15)mod 16=4 |  |  | 4 |
| 5. z5 = S4 =3 |  |  |  |

В результате первые пять значений получились следующие: 2, 4, 10, 15, 3. При необходимости получения большего количества случайных чисел можно продолжить вычисления дальше. При n=4 генерируемые числа будут иметь размер 4 бита, то есть иметь значения от 0 до 15.

В рассмотренном примере размер n слова или блока алгоритма принимался равным четырем. Это значение можно брать и другим, например 8 или 16. В случае использования n=8 таблица замен S должна состоять из 28=256 значений, а элементами таблицы замен должны быть числа от 0 до 255. Размер счетчиков i и j должен также изменить до восьми бит (максимальное значение – 255 ). Кроме того, все вычисления в случае n=8 необходимо выполнять по модулю 256. Аналогичные изменения в алгоритме необходимо производить и при других значениях параметра n.

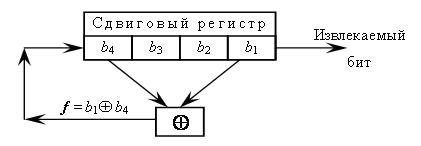
Алгоритм RC4 тщательно изучался криптоаналитиками. В нем не обнаружено каких бы то ни было слабых мест. Помимо высокой устойчивости к криптоанализу, этот алгоритм очень быстр и может использоваться для генерации ключевой последовательности при потоковом шифровании.

**Задания для самостоятельного решения**

**1.** Определите первые 16 бит псевдослучайной последовательности, получаемой с помощью генератора ПСЧ на основе линейного сдвигового регистра, изображенного на рисунке, если начальное значение регистра следующее:

а) b4=0, b3=0, b2=0, b1=1;

б) b4=1, b3=1, b2=0, b1=1.



**2.** Определите период псевдослучайных последовательностей, получаемых с помощью генератора ПСЧ на основе сдвигового регистра с обратной связью из упражнения 1.

**3.** Продолжите вычисление псевдослучайной последовательности по алгоритму RC4, начатое в задании 3. ( n=4, ключ – последовательность чисел 1, 2, 3, 4, 5, 6 ) и найдите z6, z7, z8, z9 и z10.

**4.** Произведите вычисление псевдослучайной последовательности по алгоритму RC4 (n=4) и найдите z1, z2, z3, z4 и z5. В качестве секретного ключа используйте последовательность: 4, 3, 2, 1.

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА:**

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных
2. Спирина М.С.,Спирин П.А.Дискретная математика: учебник: Рекомендовано ГОУВПО «МГТУ им. Н. Э. Баумана». — 9-e изд., испр. — 368 c., пер. No 7 бц.

**Интернет-ресурсы:**

www.intuit.ru

**Порядок представления материала:** на бумажном носителе или на сайте преподавателя.

**Срок представления материала:** семинарское занятие по теме.

**Форма контроля со стороны преподавателя:** собеседование

Критерии оценки: оценка «зачтено» ставится, если задачи решены правильно.

**ЛИСТ САМООЦЕНКИ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Уровень освоения | Задание 1 | Задание 2 | Задание 3 | Задание 4 |
| Могу помочь другим |  |  |  |  |
| Выполнил без затруднений |  |  |  |  |
| Испытывал затруднения |  |  |  |  |

# Тема «Основные положения теории чисел, используемые в криптографии с открытым ключом»

**Задание 1.** Выясните, является ли число 261360 простым и представьте его каноническое разложение.

***Методические рекомендации***

Каждое натуральное число, большее единицы, делится по крайней мере на два числа: на 1 и на само себя. Если число не имеет делителей, кроме самого себя и единицы, то оно называется простым, а если у числа есть еще делители, то составным. Единица же не считается ни простым числом, ни составным.

***Основная теорема арифметики:*** Любое натуральное число ***n***>***1*** представляется в виде произведения простых чисел, причем единственным образом:

,

Такой вид записи называется ***каноническим разложением*** числа ***n*** на простые множители.

Данное число явно имеет другие делители, например, 10 или 2, следовательно, оно простым числом не является. Разложим число на простые множители:

|  |  |
| --- | --- |
| 261360 | 2 |
| 130680 | 2 |
| 65340 | 2 |
| 32670 | 2 |
| 16335 | 3 |
| 5445 | 3 |
| 1815 | 3 |
| 605 | 5 |
| 121 | 11 |
| 11 | 11 |
| 1 |  |

Ответ: 

**Задание 2.** Определите, являются ли взаимно простыми числа а=1656 и b=1150. Если нет, то найдите их наибольший общий делитель и линейную комбинацию.

***Методические рекомендации***

Два числа называются взаимно простыми, если они не имеют ни одного общего делителя кроме единицы, т.е. их НОД=1.

Наибольший общий делитель можно найти с помощью алгоритма Евклида. Его содержание сводится к последовательному вычислению следующих равенств:

|  |  |
| --- | --- |
| a=bq1+r1, 0<r1<b;  b=r1q2+r2, 0<r2<r1;  r1=r2q3+r3, 0<r3<r2;  … … … … … … …  rn-2=rn-1qn+rn, 0<rn<rn-1;  rn-1=rnqn+1, rn=НОД(a,b); | Действие алгоритма прекращается тогда, когда полученный остаток равен нулю; последний ненулевой остаток (rn) равен наибольшему общему делителю.  Из алгоритма Евклида следует, что для любых целых чисел а и b всегда существуют числа m и n такие, что НОД(a,b) представляется в виде линейной комбинации этих чисел: ***НОД(a,b)=rn=ma+nb.*** |

Найдем НОД(1656, 1150) с помощью алгоритма Евклида.

|  |  |
| --- | --- |
| 1656=1150⋅1+506,  1150=506⋅2+138,  506=138⋅3+92,  138=92⋅1+46,  92=46⋅2;  НОД(a,b)=46; | 46=138-92=138-(506-138⋅3)=138⋅4-506=  =4⋅(1150-506⋅2)-506=4⋅1150-506⋅9=4⋅1150-  -9⋅(1656-1150)=13⋅1150-9⋅1656. |

**Задание 3.** Решить уравнения с двумя неизвестными.

а). 24х+16у=7; б). 21х-17у=5

***Методические рекомендации***

Теорема. Для того, чтобы уравнение ***ах+by=c****, a,b,c∈Z* было разрешимо необходимо и достаточно, чтобы c делилось на *НОД(a,b).*

Теорема.Все решения в целых числах уравнения ***ах+by=c*** могут быть заданы формулами:

, где t*∈Z*, а х0, у0 – частное решение уравнения.

а). Найдем НОД(24,16)=8. Проверим, делится ли 7 на НОД(24,16). Ясно, что 7 не делится на 8, следовательно, корней нет.

б). Найдем НОД(21,17)=1, 51. Данное уравнение всегда имеет решения и их бесконечно много. Используя алгоритм Евклида получаем равенства:

21=17⋅1+4

17=4⋅4+1.

Строим линейную комбинацию в виде: НОД(21,17)=21m+17n:

1=17-4⋅4=17-4⋅(21-17)=17-4⋅21+4⋅17=17⋅(1+4)-4⋅21=21⋅(-4)+17⋅5. Получили:

21⋅(-4)-17⋅(-5)=1. Умножим его на 5:

21⋅(-20)-17⋅(-25)=5. Т.о., получили частные решения х0=-20 и у0=-25.

Общее решение получим из системы:

.

**Задание 4.** Верно ли, что

* 1. 62 (mod 2);
  2. 1823618218 (mod 3);
  3. 217 (mod 2) ⇒31 (mod 2);
  4. 2014 (mod 6)⇒107 (mod 6).

***Методические рекомендации***

На множестве целых чисел можно определить бинарное ***отношение сравнимости*** ⊂Z2 следующим образом: для того, чтобы два целых ***числа*** были ***сравнимы*** по модулю m необходимо и достаточно, чтобы их разность (a-b) делилась на m или другими словами, если при делении на m они дают один и тот же остаток. Записывают (a,b)∈ или ab(mod m).

**Свойства** отношения сравнимости на множестве Z:

1). Если ab (mod m) и k∈Z, то a+kb+k (mod m).

2). Если ab (mod m) и сd (mod m), то a±cb±d (mod m).

3). Если ab (mod m) и сd (mod m), то acbd (mod m).

4). Если ab (mod m), k∈Z и n∈N, то akbk (mod m) и anbn (mod m).

5). Если akbk (mod m) и (k,m)=1 (т.е. k и m взаимно простые), то ab (mod m).

6). Если akbk (mod mk) и k∈N, то ab (mod m).

7). Если ab (mod m) и δ - общий делитель a и m, то bδ.

Итак, решение задачи 4 следующее:

а) 62 (mod 2), верно по определению т.к. 6-2=4, 42.

* 1. 1823618218 (mod 3), по определению т.к. 18236-18218=18, 183.
  2. 217 (mod 2)⇒3⋅71⋅7 (mod 2). Т.к. (7,2)=1, то по свойству 5 можем сократить сравнение, т.е. 31 (mod 2).
  3. 2014 (mod 6)⇒10⋅27⋅2 (mod 6). Вывод 107 (mod 6) неверен, т.к. (10-7) не делится на 6. Чтобы получить эквивалентное сравнение, необходимо было воспользоваться свойством 6: 2014 (mod 6)⇒10⋅27⋅2 (mod 3⋅2) ⇒107(mod 3). По определению это сравнение верно.

**Задание 5.** Найдите количество элементов в полной и приведенной системе вычетов и запишите полученные системы вычетов.

а) по модулю 6;

б) по модулю 9.

***Методические рекомендации***

Фактормножество множества целых чисел по отношению сравнимости обозначают Z/mod m=Zm. Фактормножество это множество классов эквивалентности Zm={,,…,}, где ={mk| k∈Z} - множество чисел кратных m;

={mk+1| k∈Z} - множество чисел, которые при делении на m дают остаток 1;

…

={mk| k∈Z} - множество чисел кратных, дающих остаток m-1.

Эти классы называют ***классами вычетов*** по модулю m. Множество Zm носит название ***полной системы вычетов***.

Определим на множестве Zm три операции:

: , ∈Zm полагаем, что =;

: , ∈Zm полагаем, что =;

степени:  ∈Zm полагаем, что ()n=.

Рассмотрим только такие классы вычетов, элементы которых взаимно просты с m и обозначим  - подмножество Zm. (Числа а и bназываются *взаимно простыми,* если их наибольший общий делитель равен 1). -***приведенная система вычетов***.

Число элементов *s* в приведенной системе вычетов зависит от *m*. Функция *ϕ(m)=*|| называется ***функцией Эйлера****.* Значение этой функции равно количеству элементов множества, т.е. количество натуральных чисел взаимно простых с m. Например, *ϕ*(6)=2, *ϕ*(9)=6.

Если р - простое число, то *ϕ(p)=р-1*, и вообще, *ϕ(m)<m*.

Если каноническое разложение числа , то справедливо равенство:



где *p1,..., pk —* все простые делители *m.*

**Теорема.** Если {*х1*,*х2*, …, *хs*} - приведенная система вычетов и имеется целое число *a*, взаимно простое с *m*, то {*ах1*,*ах2*, …, *ахs*} - также является приведенной системой вычетов.

В данной задаче:

а) Z6={0,1,2,3,4,5};  т.е. *ϕ*(6)=2.

б) Z9={0,1,2,3,4,5,6,7,8}, .*ϕ*(9)=6. Конечно, можно воспользоваться и формулой для вычисления *ϕ(m)*: 

**Задание 6.** Найдите остаток от деления

|  |  |
| --- | --- |
| а) числа 123∙176 на 15;  б) числа 58239 на 19; | в) числа 1423 на 19;  г) числа 2123 на 11; |

***Методические рекомендации***

**а)** В данном случае можно, конечно, перемножить два числа, потом разделить на 15 и найти остаток. Но проще воспользоваться определением операции умножения по заданному модулю:

(123∙176) (*mod15*)=123(*mod15*)∙176(*mod 15*) =(3∙11) *(mod 15)*=33 (*mod 15*)=3.

**б)** Воспользуемся определением операции степени:

58239 (*mod 19*)=(58 *mod 19*)239=1239=1.

**в)** Известно, что 14-5 (*mod 19*), кроме того, (-5)23(*mod 19*)=  
=(-5)20+2+1(*mod 19*)=((-5)4)5 (*mod 19*)⋅(-5)2 (*mod 19*)⋅(-5) (*mod 19*)=  
=(625 (*mod 19*))5⋅(25 (*mod 19*))⋅(-5 (*mod 19*))(17 (*mod 19*))5⋅6(*mod 19*)⋅(-5 (*mod 19*)) (-2)5(*mod 19*)⋅6 (*mod 19*) ⋅ (-5 (*mod 19*))=(-32(*mod 19*))⋅(-30 *mod 19*))(13(*mod 19*))⋅(11(*mod 19*))=143 (*mod 19*) 10(*mod 19*).

**г)** В подобных примерах могут пригодиться следующие теоремы:

**Теорема** (Эйлера). Если *m*∈*N* и *m*>1, *(a,m)=1*, то   (*mod m*). Однако при больших m использовать эту формулу неудобно.

**Теорема** (малая теорема Ферма). Если *р*>1 — простое число и *(a,p)=1*, то  (*mod p*).

**Теорема.** Если числа *n1,..., nk* попарно взаимно простые, число *n =n1n2…nk* —их произведение, *х* и *а* — целые числа, то х a (mod n)  .

В данном случае, *m*=11 – простое число, 2 и 11 взаимно просты. Тогда по теореме Ферма 211-1 (*mod 11*)1, т.е. 210 (*mod 11*)1. Следовательно, ((210)12∙23) (*mod 11*)=(210(*mod 11*))12∙23 (*mod 11*)=112∙8(*mod 11*)=8(*mod 11*).

**Задание 7.** Решите следующие сравнения:

|  |
| --- |
| а) 5х≡3 (mod 6);  б) 3x≡6 (mod 9); |

***Методические рекомендации***

Если НОД(a,m)=1, то сравнение *ах≡b(mod m)* имеет решение и притом единственное. Единственность решения следует понимать в смысле единственности класса чисел, которые получаются по формуле *х≡b⋅aϕ(m)-1* *(mod m)*.

Если НОД(a,m)=d и b не делится на d, то сравнение *ах≡b(mod m)* решений не имеет.

Если НОД(a,m)=d и b делится на d, то сравнение *ах≡b(mod m)* нужно свести к виду: а/х=b/(mod m/), где а/=a/d, b/=b/d, m/=m/d. Теперь НОД(a/,m/)=1 и существует единственное (частное) решение х/ по модулю m/= m/d. Но m/<m и два разных числа, попавших в один класс по модулю m/ могут быть в разных классах по модулю m. Все решения запишутся в виде: х*≡*х/+ m/t, t=0,1,2,…,d-1.

а) 5х≡3 (mod 6);

*НОД(5,6)=1,* следовательно,имеется одно решение: х≡ b⋅aϕ(m)-1=3⋅5ϕ(6)-1≡3⋅52-1≡15≡3(mod 6). Класс чисел, удовлетворяющих этому сравнению можно записать так: х=3+6t.

б) 3x≡6 (mod 9);

*НОД(3,9)=3 и 63,* следовательно,имеется 3 различных класса решений. Согласно свойству 6 п. 6.1.3 можно разделить почленно это сравнение на 3: x≡2 (mod 3) – получили частное решение. Общее же решение будет выглядеть так: х1≡2(mod 9), x2≡2+3⋅1(mod 9), x3≡2+3⋅2(mod 9).

Ответ: а) х=3+6t; б) х1=2+9t, х1=5+9t, х1=8+9t.

**Задания для самостоятельного решения**

**1.** Определите, являются ли простыми числа 37, 59, 67, 93, 101, 111, 231. Представьте их в каноническом виде.

**2.** Определите, являются ли взаимно простыми числа:

а) 16 и 37;

б) 16, 37 и 38;

в) 5, 9, 27 и 54;

г) 2, 4, 7, 15, 59.

**3.** Определите число натуральных чисел, не превосходящих 59 и, взаимно простых с 59.

**4.** Определите число натуральных чисел, не превосходящих 143 и, взаимно простых с 143.

**5.** Найдите наибольший общий делитель двух чисел a и b, используя алгоритм Евклида. Составьте линейную комбинацию. Пару чисел взять из Приложения 2 согласно номеру по списку в журнале.

6. Решить уравнения с двумя неизвестными. Уравнение взять из Приложения 3 согласно номеру по списку в журнале.

**7.** Найдите количество элементов в полной и приведенной системе вычетов

|  |  |
| --- | --- |
| а) по модулю 60;  б) по модулю 81;  в) по модулю 5; | г) по модулю 5040;  д) по модулю 1294700  е) по модулю 100. |

**8.** Вычислите

|  |  |  |
| --- | --- | --- |
| а) 38 mod 10  б) 38 \* 57 mod 11. | в) 7347 mod 23;  г) 7308 mod 9; | д) 13257 mod 6  е) 7500 mod 5 |

**9.** Найдите остатки от деления чисел. Числа взять из Приложения 4 согласно номеру по списку в журнале.

**10.** Решите сравнение. Сравнение взять из Приложения 5 согласно номеру по списку в журнале.

**11.** Вычислите

а) 7-1 mod 10

б) 3-1 mod 11

***Примечание:*** 7-1≠1/7. 7-1 – это число, обратное числу 7 по заданному модулю, т.е. произведение 7-1 \*7 должно быть равно единице по заданному модулю. По сути 7-1 – это решение сравнения вида 7х≡1 (mod 10).

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА:**

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных
2. Спирина М.С., Спирин П.А.Дискретная математика: учебник: Рекомендовано ГОУВПО «МГТУ им. Н. Э. Баумана». — 9-e изд., испр. — 368 c.

**Интернет-ресурсы:**

www.intuit.ru

**Порядок представления материала:** на бумажном носителе или на сайте преподавателя.

**Срок представления материала:** семинарское занятие по теме.

**Форма контроля со стороны преподавателя:** собеседование

Критерии оценки: оценка «зачтено» ставится, если задачи решены правильно.

**ЛИСТ САМООЦЕНКИ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Уровень освоения | Задание 1 | Задание 2 | Задание 3 | Задание 4 | Задание 5 | Задание 6 |
| Могу помочь другим |  |  |  |  |  |  |
| Выполнил без затруднений |  |  |  |  |  |  |
| Испытывал затруднения |  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Уровень освоения | Задание 7 | Задание 8 | Задание 9 | Задание 10 | Задание 11 |
| Могу помочь другим |  |  |  |  |  |
| Выполнил без затруднений |  |  |  |  |  |
| Испытывал затруднения |  |  |  |  |  |

# Тема «Криптографические алгоритмы с открытым ключом и их использование»

**Задание 1.** Проиллюстрируйте алгоритм RSA передачи сообщения от пользователя А пользователю Б сообщение. Пусть им выбраны, например, следующие параметры: Р = 3, Q= 11.

***Методические рекомендации***

Алгоритм RSA представляет собой блочный алгоритм шифрования, где зашифрованные и незашифрованные данные должны быть представлены в виде целых чисел между 0 и n -1 для некоторого n.

Итак, пусть абонент А хочет передать зашифрованное сообщение абоненту Б. В этом случае абонент Б должен подготовить пару (открытый ключ; закрытый ключ) и отправить свой открытый ключ пользователю А.

Первым этапом является генерация открытого и закрытого ключей. Для этого Б вначале выбирает два больших простых числа Р и Q. Затем вычисляется произведение N:

N = PQ. После этого определяется вспомогательное число f:

f = (Р - l)(Q - 1). Т.е. f = (Р - l)(Q - 1) = (3-1)(11-1) = 20.

Затем пользователь Б выбирает любое число d случайным образом такое, что d < f и взаимно простое с f (это необходимо для того, чтобы зашифрованное сообщение можно было потом однозначно восстановить). Пусть d = 13. Это число будет одним из компонентов открытого ключа.

Далее необходимо найти число е, которое можно будет использовать в качестве закрытого ключа для расшифрования сообщения. Значение е должно удовлетворять соотношению: еd = 1 (mod f)

Числа d и N будут открытым ключом пользователя, а значение е – закрытым ключом.

Для малых значений f число е можно найти подбором. Решение такого сравнениярассмотрено в задаче 7 предыдущей темы. В нашем случае подходит е=17. (Проверяем: 13\*17 mod 20 = 221 mod 20 = 1.)

Теперь пользователь Б должен запомнить свой закрытый ключ 17, отправить открытый ключ (13, 33) пользователю А и уничтожить числа Р = 3 и Q = 11.

Пользователь А, получивший открытый ключ (13, 33), увидев, что N=33, разбивает исходное сообщение на три блока, причем значение каждого меньше N. Например, пусть имеется три блока m1=8, m2=27, m3,=5. Затем пользователь А шифрует каждый блок:

c1=813 mod 33 = 17

c2 = 2713 mod 33 = 15

c3 = 513 mod 33 = 26

Зашифрованное сообщение, состоящее из трех блоков (17, 15, 26), передается пользователю Б, который, используя свой закрытый ключ е = 17 и N=33, расшифровывает сообщение:

m1 = 1717 mod 33 = 8

m2 = 1517 mod 33 = 27

m3 = 2617 mod 33 = 5

Таким образом, абонент Б расшифровал сообщение от абонента А.

**Задание 2.** Проиллюстрируйте алгоритм Диффи-Хеллмана обмена ключами между пользователями 1 и 2. Пусть ими выбраны, например, следующие общие параметры: Р = 11, А = 7.

***Методические рекомендации***

Алгоритм Диффи-Хеллмана не применяется для шифрования сообщений или формирования электронной подписи. Он позволяет двум или более пользователям обменяться без посредников ключом, который может быть использован затем для симметричного шифрования. Схема открытого распределения ключей, предложенная Диффи и Хеллманом, произвела настоящую революцию в мире шифрования, так как снимала основную проблему классической криптографии – проблему распределения ключей.

Алгоритм основан на трудности вычислений дискретных логарифмов. В этом алгоритме, как и во многих других алгоритмах с открытым ключом, вычисления производятся по модулю некоторого большого простого числа Р.

**Этап 1.** Вначале специальным образом подбирается некоторое натуральное число А, меньшее Р.

Для того, чтобы алгоритм Диффи-Хеллмана работал правильно, то есть оба пользователя, участвующих в протоколе, получали одно и то же число Z, необходимо правильным образом выбрать число А, используемое в вычислениях. Число А должно обладать следующим свойством: все числа вида

A mod P, A2 mod P, A3 mod P,... , AP-1 mod P

должны быть различными и состоять из целых положительных значений в диапазоне от 1 до Р-1 с некоторыми перестановками. Только в этом случае для любого целого Y < Р и значения A можно найти единственную экспоненту Х, такую, что

Y = AХ mod P, где 0 <= X <= (P - 1)

При произвольно заданном Р задача выбора параметра А может оказаться трудной задачей, связанной с разложением на простые множители числа Р-1. На практике можно использовать следующий подход, рекомендуемый специалистами. Простое число Р выбирается таким, чтобы выполнялось равенство Р = 2q + l, где q — также простое число. Тогда в качестве А можно взять любое число, для которого справедливы неравенства

1<A<P-1 и Aq mod P ≠ 1

**Этап 2.** Если мы хотим зашифровать значение X, то вычисляем

Y = AX mod P.

Причем, имея Х, вычислить Y легко. Обратная задача вычисления X из Y является достаточно сложной. Экспонента X как раз и называется дискретным логарифмом Y. Таким образом, зная о сложности вычисления дискретного логарифма, число Y можно открыто передавать по любому каналу связи, так как при большом модуле P исходное значение Х подобрать будет практически невозможно. На этом математическом факте основан алгоритм Диффи-Хеллмана для формирования ключа.

Пусть два пользователя, которых условно назовем пользователь 1 и пользователь 2, желают сформировать общий ключ для алгоритма симметричного шифрования. Вначале они должны выбрать большое простое число Р и некоторое специальное число А, 1 < A < P-1, такое, что все числа из интервала [1, 2, ..., Р-1] могут быть представлены как различные степени А mod Р. Эти числа должны быть известны всем абонентам системы и могут выбираться открыто. Это будут так называемые общие параметры. В данной задаче Р = 11, А = 7.

Затем первый пользователь выбирает число Х1 (X1<P), которое желательно формировать с помощью датчика случайных чисел. Это будет закрытый ключ первого пользователя, и он должен держаться в секрете. На основе закрытого ключа пользователь 1 вычисляет число

Y_1 = A^{X_1}\: mod \: P, которое он посылает второму абоненту.

Аналогично поступает и второй пользователь, генерируя Х2 и вычисляя

Y_2 = A^{X_2}\: mod \: P. Это значение пользователь 2 отправляет первому пользователю.

После этого у пользователей должна быть информация, указанная в следующей таблице:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Общие параметры | Открытый ключ | Закрытый ключ |
| Пользователь 1 | Р, А | Y1 | Х1 |
| Пользователь 2 | Y2 | Х2 |

Пусть выбраны Х1 = 3, Х2= 9.

Вычисляем Y1 = 73 mod 11 = 2 и Y2= 79 mod 11 = 8.

**Этап 3.** Затем пользователи обмениваются открытыми ключами Y1 и Y2. И из чисел Y1 и Y2, а также своих закрытых ключей каждый из абонентов может сформировать общий секретный ключ Z для сеанса симметричного шифрования. Вот как это должен сделать первый пользователь:

Z = (Y_2)^{X_1}\: mod \: P

Никто другой кроме пользователя 1 этого сделать не может, так как число Х1 секретно. Второй пользователь может получить то же самое число Z, используя свой закрытый ключ и открытый ключ своего абонента следующим образом:

Z = (Y_1)^{X_2}\: mod \: P

Если весь протокол формирования общего секретного ключа выполнен верно, значения Z у одного и второго абонента должны получиться одинаковыми.

Пользователь 1: Z = 83 mod 11 = 6.

Пользователь 2: Z = 29 mod 11 = 6.

Теперь они имеют общий ключ 6, который не передавался по каналу связи и который пользователи 1 и 2 могут использовать значение Z в качестве секретного ключа для шифрования и расшифрования данных.

Самое важное, что противник, не зная секретных чисел Х1 и Х2, не сможет вычислить число Z. Не зная Х1 и Х2, злоумышленник может попытаться вычислить Z, используя только передаваемые открыто Р, А, Y1 и Y2. Безопасность формирования общего ключа в алгоритме Диффи-Хеллмана вытекает из того факта, что, хотя относительно легко вычислить экспоненты по модулю простого числа, очень трудно вычислить дискретные логарифмы. Для больших простых чисел размером сотни и тысячи бит задача считается неразрешимой, так как требует колоссальных затрат вычислительных ресурсов.

**Задание 3.** Проиллюстрируйте алгоритм Эль-Гамаля передачи сообщения m=9 от пользователя А пользователю Б сообщение. Пусть им выбраны, например, следующие общие параметры: Р = 11, А = 7.

***Методические рекомендации***

Асимметричный алгоритм, предложенный в 1985 году Эль-Гамалем (T. ElGamal), универсален. Он может быть использован для решения всех трех основных задач: для шифрования данных, для формирования цифровой подписи и для согласования общего ключа.

Безопасность этого алгоритма, так же как и алгоритма Диффи-Хеллмана, основана на трудности вычисления дискретных логарифмов. Этот алгоритм фактически использует схему Диффи-Хеллмана, чтобы сформировать общий секретный ключ для абонентов, передающих друг другу сообщение, и затем сообщение шифруется путем умножения его на этот ключ.

**Этап 1.** И в случае шифрования, и в случае формирования цифровой подписи каждому пользователю необходимо сгенерировать пару ключей. Для этого, так же как и в схеме Диффи-Хеллмана, выбираются некоторое большое простое число Р и число А, такие, что различные степени А представляют собой различные числа по модулю Р. Числа Р и А могут передаваться в открытом виде и быть общими для всех абонентов сети.

Затем каждый абонент группы выбирает свое секретное число Хi из интервала *(1,P)*, взаимно простое с *P-1* и вычисляет соответствующее ему открытое число . Таким образом, каждый пользователь может сгенерировать закрытый ключ Хi и открытый ключ Yi.

Общие параметры заданы Р=11, А=7.

Пользователь 1 выбирает Х1=3 - случайное целое число из интервала (1,11), взаимно простое с 10 и вычисляет Y1= 73 mod 11=2.

Открытый ключ - тройка (A, P ,Y1) передается пользователю 2 для выполнения шифрования, а закрытый ключ — число Х1 – хранится в тайне.

Пользователь 2 выбирает закрытый ключ Х2 = 9 и вычисляет открытый ключ Y2 = 79mod 11 = 8.

Открытый ключ - тройка (A, P ,Y2) передается пользователю 1 для выполнения шифрования, а закрытый ключ — число Х2 – хранится в тайне.

**Этап 2.** Теперь рассмотрим, каким образом производится шифрование данных. Сообщение, предназначенное для шифрования, должно быть представлено в виде одного числа или набора чисел, каждое из которых меньше Р. Пусть пользователь 1 хочет передать пользователю 2 сообщение m=9. В этом случае последовательность действий следующая.

Пользователь 1 выбирает случайное число k, взаимно простое с Р-1, и вычисляет числа

где Y2 – открытый ключ пользователя 2. Число k держится в секрете.

Пусть k=7. Вычисляем число r = Ak mod P = 77 mod 11 = 823543 mod 11=6.

Вычисляем число e=M\*Y2k mod P=9\*87 mod 11=9 \*2097152 mod 11=7.

Пара чисел (r, е)= (6, 7), являющаяся шифртекстом, передается второму пользователю.

Второй пользователь, получив (r,e), для расшифрования сообщения вычисляет

, где Х2 – закрытый ключ пользователя 2.

В результате он получает исходное сообщение m=9.

Если злоумышленник узнает или перехватит Р, А, Y2, r, e, то он не сможет по ним раскрыть m. Это связано с тем, что противник не знает параметр k, выбранный первым пользователем для шифрования сообщения m. Вычислить каким-либо образом число k практически невозможно, так как это задача дискретного логарифмирования. Следовательно, злоумышленник не может вычислить и значение m, так как m было умножено на неизвестное ему число. Противник также не может воспроизвести действия законного получателя сообщения (второго абонента), так как ему не известен закрытый ключ Х2 (вычисление Х2 на основании Y2 — также задача дискретного логарифмирования).

По аналогичному алгоритму может производиться и согласование ключа, используемого для симметричного шифрования больших объемов данных. Более того, алгоритм Эль-Гамаля на практике целесообразно использовать именно для согласования общего ключа сессии, а не прямого шифрования больших сообщений. Это связано с тем, что в алгоритме используются операции возведения в степень и умножения по большому модулю. Так же как и в алгоритмах RSA и Диффи-Хеллмана, операции производятся над большими, состоящими из нескольких сотен или тысяч бит, числами. Поэтому шифрование больших сообщений производится крайне медленно.

**Задания для самостоятельного решения**

**1.** Пусть пользователь А хочет передать пользователю Б сообщение m=10, зашифрованное с помощью алгоритма RSA. Пользователь Б имеет следующие параметры: P=7, Q=11, d=47. Опишите процесс передачи сообщения m пользователю Б.

**2.** Пользователю системы RSA с параметрами N = 33, d = 3 передано зашифрованное сообщение c = 13. Расшифруйте это сообщение, взломав систему RSA пользователя.

**3.** Вычислите закрытые ключи Y1, Y2 и общий ключ Z для системы Диффи-Хеллмана с параметрами А=3, Р=7, Х1=3, Х2=6.

**4.** В системе связи, применяющей шифр Эль-Гамаля, пользователь 1 желает передать сообщение m пользователю 2. Найдите недостающие параметры при следующих заданных параметрах P = 19, A = 2, Х2 = 3, k = 5, m = 10.

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА:**

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных
2. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма
3. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования
4. ГОСТ Р34.10-2001. Процессы формирования и проверки электронной цифровой подписи  
   **Интернет-ресурсы:**

www.intuit.ru

**Порядок представления материала:** на бумажном носителе или на сайте преподавателя.

**Срок представления материала:** семинарское занятие по теме.

**Форма контроля со стороны преподавателя:** собеседование

Критерии оценки: оценка «зачтено» ставится, если задачи решены правильно.

**ЛИСТ САМООЦЕНКИ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Уровень освоения | Задание 1 | Задание 2 | Задание 3 | Задание 4 |
| Могу помочь другим |  |  |  |  |
| Выполнил без затруднений |  |  |  |  |
| Испытывал затруднения |  |  |  |  |

# Тема «Электронная цифровая подпись»

**Задание 1.** Вычислить и проверить цифровую подпись, сформированную по стандарту ГОСТ Р34.10-94 одного из пользователей системы связи, который хочет подписать свое сообщение, хеш-функция которого равна 9 для передачи другому пользователю. Известно, что абоненты, обменивающиеся через Интернет зашифрованными сообщениями, имеют следующие общие параметры: Р = 23, Q=11, А = 6.

***Методические рекомендации***

В России принят стандарт ГОСТ Р34.10-94 "Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма".

**1.** Вначале для группы абонентов выбираются три общих (несекретных) параметра Р, Q и A, которые должны удовлетворять следующим требованиям:

* параметр Р должен быть простым числом длиной от 512 до 1024 бит. Старший бит в р должен быть равен единице.
* Q – простое число длиной 254-256 бит, Q должно быть делителем числа (р-1). Старший бит в Q должен быть равен единице.
* число А, удовлетворяющее неравенству 1 < A < P-1 и являющееся корнем уравнения AQ mod P = 1.

Параметры, заданные в условии задачи верные: если P = 23, Q = 11, A =6 , то 611 mod 23 = 1 – верное равенство.

**2.** Затем каждый пользователь может сформировать закрытый и открытый ключи. В качестве закрытого ключа выбирается произвольное число Х, 0 < X < Q. Открытым ключом является число Y, получаемое по формуле

Y = АX mod P.

Предположим, пользователь А выбрал в качестве закрытого ключа число Х=8.

После этого он вычисляет открытый ключ по формуле Y = АX mod P = 68 mod 23 = 18.

**3.** Для создания каждой новой подписи каждый раз выбирается новое случайное число k, 0 < k < q.

Для создания подписи пользователь А выбирает случайное число k = 5.

Пусть результат вычисления хеш-функции для сообщения H(m) = 9.

Подпись сообщения состоит из двух чисел (r, s):

Таким образом, подпись сообщения состоит из пары чисел (r, s) = (2, 6).

**4.** Проверка подписи.

Получив сообщение вместе с подписью (2, 6), получатель вычисляет

Так как v = r, то подпись считается верной.

В 2001 г. был принят новый отечественный стандарт на алгоритм формирования и проверки ЭЦП. Его полное название следующее: "ГОСТ Р34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".

В основе ГОСТ Р34.10-2001 лежат алгоритмы с использованием операций на эллиптических кривых. Стойкость ГОСТ Р34.10-2001 основывается на сложности взятия дискретного логарифма в группе точек эллиптической кривой, а также на стойкости хэш-функции по ГОСТ Р34.11-94. Размер формируемой цифровой подписи – 512 бит.

В целом алгоритм вычислений по алгоритму ГОСТ Р34.10-2001 аналогичен применяемому в предыдущем стандарте ГОСТ Р34.10-94. Сначала генерируется случайное число k, с его помощью вычисляется компонента r подписи. Затем на основе компоненты r, числа k, значения секретного ключа и хэш-значения подписываемых данных формируется s-компонента ЭЦП. При проверке же подписи аналогичным образом проверяется соответствие определенным соотношениям r, s, открытого ключа и хэш-значения информации, подпись которой проверяется. Подпись считается неверной, если соотношения неверны.

Старый ГОСТ Р34.10-94 не отменен, и в настоящее время параллельно действуют два отечественных стандарта на ЭЦП. Однако необходимо отметить, что для прежнего ГОСТа принято ограничение: при реализации ЭЦП по стандарту ГОСТ Р34.10-94 разрешено использовать только 1024-битные значения параметра P.

Использование математического аппарата группы точек эллиптической кривой в новом ГОСТ Р34.10-2001 позволяет существенно сократить порядок модуля P без потери криптостойкости. Так, в стандарте указано, что длина числа Р может быть 256 или больше бит.

**Задание 2.** Вычислить цифровую подпись, сформированную по алгоритму Эль-Гамаля одного из пользователей системы связи, который хочет подписать свое сообщение m=5 для передачи другому пользователю. Известно, что абоненты, обменивающиеся через Интернет зашифрованными сообщениями, имеют следующие общие параметры: Р = 11, А = 7.

***Методические рекомендации***

Алгоритм Эль-Гамаля также можно использовать для формирования цифровой подписи. Группа пользователей выбирает общие параметры Р и А. Затем каждый абонент группы выбирает свое секретное число Хi, 1 < Хi< Р-1, и вычисляет соответствующее ему открытое число Y_i \: : \: Y_i=A^{X_i} \: mod \: P. Таким образом, каждый пользователь получает пару (закрытый ключ; открытый ключ) = (Хi, Yi). Открытые ключи пользователей могут храниться в общей базе системы распределения ключей и при необходимости предоставляться всем абонентам системы.

Сообщение, предназначенное для подписи, должно быть представлено в виде числа, меньшего модуля Р. При большом размере сообщение разбивается на блоки необходимого размера. В некоторых случаях подписывается не само сообщение, а значение хеш-функции от него. В любом варианте цифровая подпись вычисляется в зависимости от некоторого числа m (m < P).

Пусть пользователь 1 хочет подписать свое сообщение цифровой подписью и передать его пользователю 2. В этом случае алгоритм действий следующий.

**1.** Вначале он должен выбрать себе закрытый ключ, например, Х1=3 и сформировать открытый ключ Y1 = 73 mod 11 = 2. Открытый ключ может быть передан всем заинтересованным абонентам или помещен в базу данных открытых ключей системы связи.

**2.** Затем пользователь выбирает случайное секретное число k, взаимно простое с Р-1. Пусть k=9 ( 9 не имеет общих делителей с 10 ). Далее необходимо вычислить число

**3.** Затем с помощью алгоритма Евклида необходимо найти значение b в следующем уравнении:

Решением последнего уравнения будет значение b=9.

Таким образом, пара чисел (a, b) = (8, 9) будет цифровой подписью сообщения m=5.

**4.** Сообщение m вместе с подписью (a, b) отправляется пользователю 2.

**5.** Пользователь 2 получает сообщение m и с использованием открытого ключа первого абонента Y1 вычисляет два числа по следующим формулам:

Так как с1 =с2, то цифровая подпись первого пользователя верная. Для подписывания каждого нового сообщения должно каждый раз выбираться новое значение k.

Подписи, созданные с использованием алгоритма Эль-Гамаля, называются *рандомизированными*, так как для одного и того же сообщения с использованием одного и того же закрытого ключа каждый раз будут создаваться разные подписи (a,b), поскольку каждый раз будет использоваться новое значение k. Подписи, созданные с применением алгоритма RSA, называются *детерминированными*, так как для одного и того же сообщения с использованием одного и того же закрытого ключа каждый раз будет создаваться одна и та же подпись.

**Задания для самостоятельного решения**

**1.** Абоненты некоторой сети применяют цифровую подпись по стандарту ГОСТ Р34.10-94 с общими параметрами p = 47, q = 23, a = 37. Найдите открытый ключ абонента Петрова для Х = 8.

**2.** Абоненты некоторой сети применяют цифровую подпись по стандарту ГОСТ Р34.10-94 с общими параметрами p = 47, q = 23, a = 7. Найдите открытый ключ абонента Петрова и вычислите его цифровую подпись для Х = 8, k = 7, h = 10.

**3.** Абоненты некоторой сети применяют цифровую подпись по алгоритму Эль-Гамаля с общими параметрами Р = 17, А = 3. Найдите открытый ключ абонента Петрова для Х = 11.

**4.** Абоненты некоторой сети применяют цифровую подпись по алгоритму Эль-Гамаля с общими параметрами Р = 17, А = 3. Найдите открытый ключ абонента Петрова и вычислите его цифровую подпись для Х = 3, k = 7, m = 11.

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА:**

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования данных
2. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма
3. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования
4. ГОСТ Р34.10-2001. Процессы формирования и проверки электронной цифровой подписи  
   **Интернет-ресурсы:**

www.intuit.ru

**Порядок представления материала:** на бумажном носителе или на сайте преподавателя.

**Срок представления материала:** семинарское занятие по теме.

**Форма контроля со стороны преподавателя:** собеседование

Критерии оценки: оценка «зачтено» ставится, если задачи решены правильно.

**ЛИСТ САМООЦЕНКИ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Уровень освоения | Задание 1 | Задание 2 | Задание 3 | Задание 4 |
| Могу помочь другим |  |  |  |  |
| Выполнил без затруднений |  |  |  |  |
| Испытывал затруднения |  |  |  |  |

# Тема «Совершенно секретные системы»

**Задание 1.** Определите количество информации, которое несет отдельное сообщение, состоящее из одной буквы, если источник генерирует сообщения, состоящие из одиночных букв русского языка, в алфавите которого 33 буквы.

***Методические рекомендации***

Очевидно, что информационная ценность некоторого сообщения связана с разнообразием вариантов генерируемых сообщений, или, другими словами, с разнообразием состояний источника информации. Ввиду этого можно считать, что объем информации, передаваемый отдельным сообщением, пропорционален общему числу N различных сообщений (или числу состояний источника информации). На практике, однако, в качестве меры информационной емкости принимается не само число N, а логарифм по основанию 2 от него: .

Данная формула позволяет получить результат в битах. Подобная мера получила название формально-логической логарифмической меры информации, или *меры информации по Хартли*.

Мы рассматриваем источник, который генерирует сообщения, состоящие из одиночных букв русского языка, в алфавите которого 33 буквы. Определим, сколько информации несет отдельное сообщение, состоящее из одной буквы:

.

**Задание 2.** Посчитайте количество информации по Хартли, приходящееся на сообщение из четырех букв русского алфавита.

***Методические рекомендации***

В русском алфавите 33 буквы. Определим количество информации, которое несет отдельное сообщение, состоящее из одной буквы:

.

Для определения количества информации в некотором сообщении надо количество символов в нем умножить на количество информации, содержащееся в одном символе, то есть на его информационный вес. Подсчитаем, какое количество информации несет сообщение, состоящее из четырех букв русского алфавита:

.

Таким образом, при алфавитном подходе объем информации в сообщении оценивается не по смыслу сообщения, а по статистическим характеристикам (количеству символов).

**Задание 3.** Сравните неопределенность, возникающую при вынимании шаров из урны, где находится один черный и один белый шар и неопределенность, возникающую при вынимании шаров из урны, где находятся семь черных шаров и один белый. Какая из неопределенностей больше?

***Методические рекомендации***

Так как ценность информации заключается в устранении имеющейся неопределенности, сообщения, имеющие высокую вероятность, менее ценны. Их можно в какой-то степени предвидеть заранее. И наоборот, маловероятные сообщения представляют большую ценность.

Количественная оценка информации, учитывающая вероятности генерации конкретных сообщений называется мерой информации по Шеннону.

Согласно этому методу состояние источника информации до получения сообщения потребителем характеризуется некоторой неопределенностью. При этом получение информации снимает эту неопределенность (полностью или частично):

где H нач – неопределенность, характеризующая источник сообщений до получения сообщения, а Н кон – неопределенность после получения сообщения.

Неопределенность состояния источника информации оценивается по формуле

где p i – вероятность i-го состояния источника. Знак "минус" перед суммой введен потому, что величины вероятностей являются правильными дробями и имеют отрицательные логарифмы, а оценку неопределенности нужно получить со знаком "плюс".

При вынимании шаров из урны, где находится один черный и один белый шар, неопределенность составляет

Неопределенность оказалась равной одному биту.

При вынимании шаров из урны, где находится семь черных шаров и один белый. На этот раз неопределенность составит

Мера неопределенности уменьшилась почти вдвое по сравнению с первым примером.

Вывод: неопределенность достигает максимального значения при равенстве вероятностей каждого из состояний друг другу и уменьшается с увеличением разброса этих вероятностей. Также следует заметить, что при равенстве вероятностей между собой p_i=p_j, \forall i,j=\overline{0 \dots N-1}, мера информации по Шеннону совпадает с мерой информации по Хартли.

**Задание 4.** Определите энтропию трех источников сообщений, каждый из которых может генерировать только по два разных сообщения m1 и m2. Известно, что для первого источника вероятность появления первого сообщения р(m1)=0, а вероятность второго сообщения р(m1)=1. Для второго источника вероятности сообщений равны, то есть р(m1)=0,5 и р(m2)=0,5. Для третьего источника вероятности сообщений следующие: р(m1)=0,9 и р(m1)=0,1.

***Методические рекомендации***

Пусть источник сообщений может создавать n разных сообщений m 1 , m 2 , ... m n с вероятностями p 1 , p 2 ,... , p n . В этом случае энтропия сообщения будет определяться формулой

Так как в данной формуле используется двоичный логарифм, то энтропия измеряется в битах, что общепринято в криптографии, теории информации и в компьютерных науках.

Определим энтропию каждого из источников сообщений. Для первого источника:

Энтропия или неопределенность первого источника равна нулю. И действительно, если заранее известно, что из двух сообщений всегда генерируется только одно, то никакой неопределенности нет.

Определим энтропию второго источника:

Неопределенность оказалась равной одному биту. Найдем теперь энтропию третьего источника:

Неопределенность у третьего источника меньше, чем у второго, так как из двух возможных сообщений, генерируемых третьим источником, одно более вероятно, чем другое.

Понятие энтропии играет важную роль во многих задачах теории передачи и хранения информации. В частности, энтропия может использоваться для определения максимальной степени сжатия данных. Точнее, если источник сообщений порождает текст достаточно большой длины n с определенной предельной энтропией h на бит сообщения, то этот текст теоретически может быть сжат до величины n\*h бит. Например, если h = 1/2, то текст может сжиматься вдвое и т.д. Значение n\*h является пределом и на практике достигается редко.

С точки зрения криптографии, энтропия определяет количество символов, которые необходимо раскрыть, чтобы узнать содержание сообщения. Так, если некоторый 8-битовый блок данных хранит одно из двух возможных сообщений (например, ответы "Да" или "Нет"), то достаточно правильно узнать один бит, чтобы определить значение исходного сообщения. Сколько бы бит мы не отводили для шифрования слов "Да" и "Нет", энтропия или неопределенность всегда будет меньше или равна 1.

**Задание 5.** Выполните шифрование по методу одноразовой ленты для сообщения m, которое содержит следующие двоичные цифры: m = 1100101110. В качестве ключевой используется последовательность: k = 1001100111.

***Методические рекомендации***

Выполним шифрование по методу одноразовой ленты, сложив цифры в каждом столбике по модулю 2:

|  |  |
| --- | --- |
| исходный текст | m = 1100101110 |
| биты ключевой послед-ти | k = 1001100111 |
| зашифрованный текст | с = 0101001001 |

Этот процесс напоминает наложение гаммы на поток входных данных. Шифр с одноразовой лентой действительно является гаммированием, однако, в отличие от всех рассмотренных до этого криптосистем в нем предполагается бесконечная гамма.

В одноразовой ленте все буквы встречаются с одинаковой частотой. Поэтому, сколько бы знаков гаммы нам ни было известно, мы не сможем предсказать, какой будет следующая буква. Из этого следует, что все последовательности знаков гаммы равновероятны. Это означает, что сообщение, зашифрованное с помощью шифра Вернама, может быть "дешифровано" в любой открытый текст подходящей длины, поскольку предполагаемая последовательность знаков гаммы не имеет никаких свойств, позволяющих отличить её от любой другой.

**Задание 6.** Рассчитайте расстояние единственности для шифра простой замены, применяемого к русскому языку.

***Методические рекомендации***

Шеннон ввел понятие *расстояния единственности шифра* (или *расстояния уникальности*) U, которое показывает, сколько букв зашифрованного сообщения необходимо перехватить для однозначного восстановления ключа.

Для вычисления расстояния единственности необходимо знать энтропию ключа Н(К). Для симметричных шифров энтропия ключа примерно равна логарифму числа ключей NK по основанию 2:

В нашем примере, для шифра простой замены, применяемого к русскому языку, число возможных ключей определяется количеством всех возможных таблиц замен и равно

.

Поэтому энтропия ключа будет равна

Если нам известна энтропия ключа Н(К) для некоторого шифра, то расстояние единственности U для него вычисляется по формуле

Рассчитаем расстояние единственности для шифра простой замены, применяемого к сообщению на русском языке:

То есть если длина перехваченного зашифрованного сообщения превышает 35 символов, то его, скорее всего, можно будет однозначно дешифровать. А при длине зашифрованного текста меньше 35 символов возможно неоднозначное вскрытие.

**Задания для самостоятельного решения**

**1.** Определите количество информации по Хартли, приходящееся на 1 символ, если известно, что источник генерирует 32 различных символа.

**2.** Определите количество информации по Хартли, приходящееся на 10 символов, если известно, что некоторое устройство передачи данных может генерировать 256 различных символа.

**3.** Определите количество символов в алфавите источника сообщений, если известно, что для некоторого источника сообщений количество информации по Хартли, приходящееся на 1 символ, равно 6 битам.

**4.** Определите для какого источника количество информации по Шеннону, приходящееся на один символ, будет больше, если известно, что два источника генерируют по два символа, но первый источник генерирует символы с равными вероятностями, второй – с различными.

**5.** Определите энтропию источника для заданных исходных данных, если источник сообщений может генерировать n разных сообщений m1, m2, ..., mn с вероятностями p1, p2,... , pn.

а) n = 4; p1 = 0,25, p2= 0,25, p3 = 0,375, p4 = 0,125

б) n = 6; p1 = 0,0025, p2= 0,0075, p3 = 0,09, p4 = 0,2, p5= 0,5, p6 = 0,2

в) n = 4; p1= 0,25, p2= 0,1, p3 = 0,15, p4 = 0,5

**6.** Зашифруйте сообщение m шифром Вернама с ключом k:

а) m = 1001001110, k = 0100111011

б) m = 0101101110, k = 1010101011

в) m = 1111001101, k = 0110001011

**7.** Рассчитайте энтропию ключа для шифра Цезаря со сдвигом на n позиций, применяемого для сообщений на русском языке ( 32 буквы ).

**8.** Рассчитайте расстояние единственности для шифра Цезаря со сдвигом на n позиций, применяемого для сообщений на русском языке ( 32 буквы ). Избыточность сообщений на русском языке принять равной 3,5 бит на символ.

**9.** Предполагая, что все варианты ключей равновероятны и возможны, рассчитайте расстояние единственности для шифров с заданной длиной двоичного ключа N, применяемых к сообщениям, избыточность которых составляет D:

а) N=256 бит, D =3,5 ;

б) N=512 бит, D =3 ;

в) N=128 бит, D =4.

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА:**

1. Хохлов Г.И.Основы теории информации: учебник. — 320 c., пер. No 7 бц.Дата выхода: 1-е полугодие 2014 г.
2. Спирина М.С.,Спирин П.А.Дискретная математика:учебник: Рекомендовано ГОУВПО «МГТУ им. Н. Э. Баумана». — 9-e изд., испр. — 368 c., пер. No 7 бц.

**Интернет-ресурсы:**

www.intuit.ru

**Порядок представления материала:** на бумажном носителе или на сайте преподавателя.

**Срок представления материала:** семинарское занятие по теме.

**Форма контроля со стороны преподавателя:** собеседование

Критерии оценки: оценка «зачтено» ставится, если задачи решены правильно.

**ЛИСТ САМООЦЕНКИ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Уровень освоения | Задание 1 | Задание 2 | Задание 3 | Задание 4 | Задание 5 | Задание 6 |
| Могу помочь другим |  |  |  |  |  |  |
| Выполнил без затруднений |  |  |  |  |  |  |
| Испытывал затруднения |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень освоения | Задание 7 | Задание 8 | Задание 9 |
| Могу помочь другим |  |  |  |
| Выполнил без затруднений |  |  |  |
| Испытывал затруднения |  |  |  |

# ПРИЛОЖЕНИЕ 1

Варианты заданий по теме: «Криптоанализ шифра простой замены»

**1 вариант.**

58623239993129 5872629958135415 5631633972841513567715825656 56 5854297756 – 39995631 5677 32121554314876 6315521339723954 167239327262585815, 376277 5239133972393239 31625439778439213139 1672629958131554561346 1639581395161513621246313962 7215775456135662 843139325676 58636272 336212395462336258523991 996229136212463139581356. 5631633972841582563931314862 13627631391239325656 167239333139 5439531256 54 375677316258, 3937721577395415315662, 167239567754399958135439, 391352724854 3362123954625295 316237485415124862 5439778439213139581356 1639 5852397239581356 163912953362315629 56 393772153739135262 56316339728415825656, 15 1315522162 1639 15541339841513567715825656 16723956775439995813546231314876, 9516721554126231336258525676 56 56314876 167239826258583954.

**2 вариант**

39 2520348263 664635202582 86 3951743551662044 3725275135442090375125255163 912011374648 2520376151148282 6682352982912551 7451247851245946 8651447420253737, 37448231113782 514625513482253782 86 3725275135442090375125254844 4682782551145118375944, 517482352090375944 66 90822525484437 6110442018204437, 86 6120258651396686514410 66828646513510 37 66514651395163 6639599137. 564651 8620662082466659 243510183778 5135182025379120903763, 4651, 6651181420662551 3582911014294620462044 352091143756254878 376666148224513920253763, 351086513951243746821437 442551183778 3791 253778 9125203146 5161 5166255139254878 3937242078 1018355191, 2551 2582 10248214593146 2451144225511851 3925374420253759 242025254844 3951743551 662044, 665637462059, 564651 5161826674825682253782 3725275135442090375125255163 618291517420662551664637 2582 3744828246 664448661420, 82661437 5146661046664639108246 39372437442059 101835519120.

**3 вариант**

74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 62 25 34 95 29 53 59 82 27 71 29 77 99 34 27 91 17 99 71 49 99 27 15 60 32 25 50 27 17 62 27 95 27 50 25 91 32 59 77 95 29 50 25 99 59, 25 99 74 29 53 25 59 17 99 25 91 23 49 71 25 17 99 60 49 25 34 32 25 71 95 27 82 27 32 32 25 29 50 17 25 15 77 99 32 59 77 62 95 25 53 95 29 23 32 25 17 99 60 34 15 35 17 27 99 27 71 25 12 25 99 95 29 45 49 74 29. 62 95 27 63 34 27 71 17 27 12 25, 50 27 17 62 27 95 27 50 25 91 32 29 35 95 29 50 25 99 29 17 29 82 49 83 62 25 17 27 50 27 62 95 25 34 59 74 99 25 71 50 27 53 25 62 29 17 32 25 17 99 49 17 71 35 53 29 32 29 17 32 29 15 49 23 49 27 82 32 29 34 27 63 32 25 95 29 50 25 99 29 77 10 27 12 25 25 50 25 95 59 34 25 71 29 32 49 35 49 95 27 53 27 95 71 49 95 25 71 29 32 49 27 82 74 95 49 99 49 23 32 89 83 74 25 99 74 29 53 59 50 15 25 74 25 71 62 49 99 29 32 49 35 49 53 29 62 25 82 49 32 29 77 10 49 83 59 17 99 95 25 91 17 99 71. 34 15 35 62 25 17 15 27 34 32 49 83 25 62 99 49 82 29 15 60 32 25 62 95 49 82 27 32 27 32 49 27 34 49 17 74 25 71 89 83 82 29 17 17 49 71 25 71 12 25 95 35 23 27 91 53 29 82 27 32 89. 74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 95 29 50 25 99 89 34 25 17 99 49 12 29 27 99 17 35 25 62 99 49 82 49 53 29 67 49 27 91 62 95 25 12 95 29 82 82 32 25 12 25 25 50 27 17 62 27 23 27 32 49 35.

**4 вариант**

48 23 18 40 94 35 62 53 94 25 53 15 35 91 35 40 35, 52 23 52 53 40 35 94 35 40 23 94 23 91 52 94 49 24 23 84 89 94 23 64 55 53 15 18 53 91, 24 53 88 23 62 12 25 76 94 23 64 35 24 49, 35 94 49 88 53 48 94 23 24, 41 91 35 91 23 52 31 49 15 53 91. 47 91 35 41 49 62 84 91 62 35 35 91 41 23 84 91 25 31 29 24 35 64 35 27 35 88 53 94 23 91 35, 52 35 91 35 55 35 53 35 94 25 84 64 29 91 23 24, 52 35 40 15 23 48 23 62 53 55 94 49 24 48 23 49 40 35 24 25 41 49 91 89 94 53 94 23 24 53 91 53 24 94 23 15 53 62 49 12 52 49, 12 53 15 12 49 60 53 18 49 94 23 62 84 91 55 53 41 49. 53 40 35 94 35 40 23, 62 29 48 62 23 62 84 62 35 25 18 15 62 25 88 53 94 25 53 18 52 35 24 53 31 23 94 25 53 62 35 48 15 49 27 23, 64 35 24 49 41 25 24 23 35 91 55 23 88 53 94 94 29 76 84 25 40 94 23 24 35 64 55 53 64 38 91 84 91 62 25 25 94 23 64 49 91 25 25 64 35 41 91 25 62 91 49 88 53 84 53 52 49 94 15 49 49 15 23 55 25 24 23 84 89 35 31 35 41 91 35 – 91 35. 52 23 52 35 76-91 35 64 55 53 15 18 53 91 84 40 24 49 27 25 18 84 91 49 52 35 18 35 91 24 53 91 53 24 62 91 53 18 94 35 91 49.

**5 вариант**

79 61 31 96 28 35 85 52 26 30 24 21 52 85 59 49 79 30 88 79 49 30 52 79 59 85 26 30 24 21 59 85 42 79 88 61 28 35 86 50 96 28 52 30 50, 24 30 96 74 21 59 90 59 30 96 30 24 85 61 86 26 96 85 88 79 96 79 24 61 79 11 28 52 79 78 31 85, - 21 50 30 96 85 31 21 61 59 31 85 11 26 79 24 96 79 59 35 79 31 59 96 30 31 52 21 50 61 79 11 31 21 96 35 85 61 31 85, 21 26 79 78 30 50 28 67 86 85 61 30 35: 35 79 24 24 67 79 28 24 30 61, 35 96 85 61 21 24 69 21 35 90 52 30 35, 61 79 96 50 21 52 90 61 86 11 96 79 59 35, 42 24 79 96 79 49 86 11 49 30 59, 49 79 52 79 59 86 69 49 30 35 21 59 26 30 52 79 11 26 46 30 61 85 69 86, 88 79 52 28 67 86 30 88 52 21 42 21, 96 79 49 61 86 30 67 30 52 86 30 42 28 67 86, 42 21 88 79 96 30 52 79 30 52 85 69 79, 61 30 85 59 26 79 96 78 30 61 61 79 30 24 21 74 30 61 21 50 30 31 79 50 61 21 49 79 42 96 21 59 35 61 86 30 26 96 86 29 85 31 85..

**6 вариант**

56 27 54 54 27 56 51 32 82 16 63 49 27 63 11 30 73 35 23 54 89 70 27 63 27 49 32 70 35 16 97 82 16 67 73 27 51 30 56 32 63 70 29 63 27 49 32 73 29 54 73 27 48 29 13 29 82 56 82 27 95 54 27 35 27 18 51 29, 97 56 27 70 29 63 30 51 51 35 15 63 89 48 16. 16 63 15 11 51 30 82 29 49 65 27 54 32 63 30 49 29 61 27 63 32 48 30 - 27 56 51 35 15 56 30 23 32 27 11 70 27 35 27 18 32 56 29 63 89 82 30 23, 27 82 30 51 30 51 11 15 73 35 29 54 70 27 49 65 32 38 30 63 30 73 35 32 23 56 82 16 67 70 49 56 35 29 97 16. 82 27 49 51 27 13 51 29 54 30 27 82 27 73 16 49 56 32 63 70 29 63 27 49 32 73 29 54 82 15 95 16 73 27 35 32 70 15 56 30 38 32 63 32 92-73 27 54 11 30 61 30 18 82 32 51 30 49 63 27 18 29 82 82 16 67 61 30 92 29 56 16. 27 82 49 16 82 16 63 61 30 92 29 56 16 73 27 54 13 15 24 51 16 32 70 92 27 24 29 63 73 27 49 56 16 73 29 82 89 51 30 13.

**7 вариант**

34 28 68 91 13 83 10 65 27 68 49 10 26 65 27 68 75 26 39 78 53 75 83 53 18 26 36 62 91. 26 10 74 53 13 49 10 83 10 65 53 53 36 68 72 28 10 28 13 18 86 10 27 53 75 39 83 68 57 26 18 10 91 53 57 36 53 65 28 68 91 10, 83 68 75 27 13 34 13 24 13 18 53 36 74 53 36 10 74 10 36 57 36 13, 83 68 74 10 91 10 91 10 36 13 68 26 74 18 62 34 10 27 10 36 10 75 26 13 86 39 68 74 36 10. 83 18 10 34 28 10, 26 57 26 50 62 27 68 83 68 65 57 86 13. 26 57 26 49 10 83 10 65 53 34 19 13 27 53 75 39 53 34 75 13 75 68 50 68 15 83 18 68 83 53 26 10 27 53. 49 10 83 10 65 53 10 27 74 68 72 68 27 44, 83 68 28 72 68 18 13 34 80 13 72 68 91 10 75 27 10, 83 68 26 10, 75 26 10 18 68 15 68 28 13 86 28 62 53 13 96 13 27 13 74 10 18 75 26 34 - 91 13 36 26 68 27 10 53, 74 10 86 13 26 75 44, 34 10 27 13 18 39 44 36 74 53. 34 83 18 53 65 68 86 13 15 26 13 91 36 68 26 53 96 10, 53 18 44 28 68 91 23 26 68 26 28 78 75 75 10 36 28 13 18 - 34 26 44 36 57 27 72 68 27 68 34 57 34 34 68 18 68 26, 23 26 10 74 53 15 72 18 53 47 – 75 26 13 18 34 44 26 36 53 74, 86 28 57 96 53 15, 74 68 72 28 10 18 10 36 13 36 68 13 86 53 34 68 26 36 68 13 53 75 83 57 75 26 53 26 28 57 65.

**8 вариант.**

45 34 26 34 97 77 34 47 49 67 14 22 49 67 47 34 49 39 77 69 53 89 26 10 97 10 49 10 77 45 53 31 10 14 10 47 22. 17 90 56 14 34 77 67 49, 49 67 75 49 10 53 14 53 49 26 90 47 10, 77 34 39 47 56 34 31 56 26 67 52 34 13 10 84 22 53 77 34 47 49 67 14 22 49 67 28 34 84 26 67 31, 67 49 10 97 90 31 10 14 53 47 22 31 28 70 89 49 53 93 14 10 56 10 93 56 47 10, 53 45 34 84 90 26 34 93 69 58 37 28 67 31 10 70 47 84 10 14 22 77 10 70 53 89 14 10, 31 90 47 39 77 39 31 75 53 47 22, 47 14 67 31 77 67 13 10 14 67, 53 97 34 89 67 28 67 26 69 90, 31 56 26 90 47 49 53 31 10 14 10 13 34 26 84 31 34 53 97 26 70 69 77 39 58 69 67 97 39 28 67 26 24 53 70, 53 14 53 56 26 67 49 10 53 77 10. 97 10 84 34 28 39 52 53 84 67 89 67 97 31 34 26 22 49 10 52 26 67 47 10 14 53 31 56 34 45 22 69 14 70 47 13 53 89 10 77 53 70 28 39 47 67 26 10, 53 53 89 26 10 77 10 45 53 77 10 14 10 47 22 47 77 67 31 10.

**9 вариант.**

81 49 86 49 12 73 92 50 81 50 15 50 62 47 49 15 56 50 51 76 73 33 94 76 15 94 65 81 47 76. 94 76 47 49 81 47 76, 15 76 62 47 76 26 28 16 51 62 76 26 28 76 51 70 58 76 26 73 86 65 84 76 94, 47 76 15 94 65 81 47 76 15 56 50 51 76. 24 16 51 70 62 76 49 26 94 76 86 76 28 94 33 62 49 47 17 65 84 49 15 76 92 15 49 62 47 49 24 86 49 51 70 96 50 51 50. 56 76 31 73 50 47 49 62 47 76 31 76 24 76 73 65 62 50 51 33 86 49 58 33 51 15 56 50 567 0 65 62 47 16 62. 47 65, 47 50 73 76 84 49 43 76 56 70 81 56 76-56 76 73 49 51 50 56 70… 17 24 76 58 49 51 92 94 76 51 51 49 73 84. 76 94 50 12 50 92 58 33 15 70 92 94 50 28 33 47 49 56 49 65 86 49 94 56 76 86 50, 17 73 49 86 84 50 51 15 17 65 92 49 86 49 47 47 76. 86 49 94 56 76 86 76 62 28 16 51 50 62 76 51 76 73 50 17 84 49 47 96 33 47 50 28 50 51 70 12 50 94 76 92 15 94 76 31 76 92 76 12 86 50 15 56 50. 94 76 31 73 50 17 92 76 58 49 51, 76 47 50 81 56 76-56 76 15 76 15 86 49 73 76 56 76 81 49 47 47 76 24 33 15 50 51 50, 62 76 84 49 56 47 76 92 16 26 65 94 50 12.

**10 вариант.**

20 43 40 13 15 91 31 54 75 31 91 12. 88 56, 88 40 29 15 71 31 13 15 91 12 49 91 15 – 91 15 29 31 54 40 91 12… 17 15 61 69 31 44, 20 75 15 36 31 54 62 75 25 15 29 84 65 31 25 56. 90 44 15 62 40 43 40 54 65 20 88 31 17 58 65 15 62 90 26 90, 75 15-17 90 29 90 44 15 44 56, 88 31 29 40 54 31 62 90 26 49 31 54 15 17 31 62 17 91 31 44 88 58 13 15 49 62 40 13 90 17 25 15 43 15 17 15 44 36 40 25 34 90 62 31 88 40 36 31 31. 15 88 62 56 25 90 54 49 91 15-91 15 15 49 31 88 12 75 25 15 91 90 17 88 15 75 40 13 88 56 69 31 31. 29 40 71 31 17 15 88 20 84 69 31 31. 56 17 90 29 31 17 44 31 88 20, 75 25 15 29 84 65 31 25 88 31 65 62 15 54 12 62 15 44 90 88 56 91 75 15 44 56 49 40 54 65 20, 17 65 91 40 17 54 20 20 15 91 17 90 65 36 56 84 49 31 54 84 65 91 12 88 40 44 31 65 91 15, 88 15 17 65 31 71 31 17 43 20 54 65 31 61 20 17 25 56 62 90, 43 40 91 56 36 90 54 65 90 52 40 25 31 91 56 90 43 40 52 15 17 15 25 90 54.

**11 вариант.**

65 27, 67 40 58 34 11 47 27 42 27 45 82 34 11 14 49 14 89 95 47. 65 14 90 36 89 34 34 67 36 90 36 45 67 11 36 65 65 34 89 34, 11 17 82 34 67 19 24 34 95 40 45 17 34 45 82 36 24 65 14 70 25 36 82 34 90 36 73. 70 34 67 49 45 67 95 40 65 40, 17 34 45 95 36 24 14 58 34 67 34 95 34 73 34 65 14 45 36 73 90 40 45 17 95 36 59 47 11 40 82 14, 24 40 11 65 34 14 65 40 24 36 42 65 34 17 34 24 25 49 67 40 40 25 36 95 14 58 34 45 40 25 14, 69 67 34 11 45 36 42 36 45 27 11 36 95 36 65 65 40 49 24 36 95 42 40 11 40, 90 82 36 65 34 34 65, 45 58 34 36 73 45 34 11 36 67 45 58 14 73 45 34 31 63 17 34 24 24 36 95 42 14 11 40 36 67 65 34 95 25 40 82 19 65 47 36 24 14 17 82 34 25 40 67 14 90 36 45 58 14 36 34 67 65 34 32 36 65 14 49, 17 34 65 36 25 65 34 89 27 65 40 82 40 42 14 11 40 36 67 67 34 95 89 34 11 82 31, 17 95 14 45 47 82 40 36 67 65 40 89 40 45 67 95 34 82 14 59 40 82 36 67 65 47 36 67 95 27 17 17 47 14 34 59 25 36 65 14 11 40 36 67 45 49 17 95 34 18 45 34 31 63 65 47 25 14 24 36 82 36 89 40 56 14 49 25 14. 40 17 34 67 34 25 27 63 24 36 45 19 65 14 58 40 58 65 36 17 34 82 40 89 40 36 67 45 49 65 36 82 36 89 40 82 19 65 34 17 95 36 59 47 11 40 67 19 45 34 11 36 67 45 58 14 25 59 34 36 11 47 25 17 82 34 11 56 40 25, “25 34 95 45 58 14 25 24 19 49 11 34 82 40 25”. 36 42 36 82 14 90 67 34 - 45 58 40 65 24 40 82 95 40 63 89 34 95 14 67 45 49 17 34 17 34 82 65 34 73…

**12 вариант.**

14 70 14 65 36 59 47 82 34, 40 58 40 58 42 36. 17 95 34 45 67 34-65 40 17 95 34 45 67 34 32 36 45 67 36 95 34 25 27 42 14 58 34 11, 65 40 11 14 24 - 45 67 40 65 24 40 95 67 65 47 36 36 11 95 34 17 36 34 14 24 47, 45 63 40 17 40 24 65 34 89 36 95 25 40 65 45 58 14 25 14 40 11 67 34 25 40 67 40 25 14, 14 67 40 82 19 49 65 45 58 14 25 14 40 58 11 40 82 40 65 89 40 25 14, 32 11 36 24 45 58 14 25 14 59 40 63 27 58 40 25 14, 59 36 82 19 89 14 73 45 58 14 25 14 25 14 65 40 25 14, 18 95 40 65 56 27 63 45 58 14 25 14 45 14 89 40 95 36 67 40 25 14 14 32 11 36 73 56 40 95 45 58 14 25 14 90 40 45 40 25 14. 17 95 36 24 25 36 67 47 45 65 40 95 49 42 36 65 14 49, 11 63 49 67 47 36 17 34 34 67 24 36 82 19 65 34 45 67 14, 25 34 42 65 34 59 36 63 34 45 34 59 47 70 70 82 34 17 34 67 17 95 14 34 59 95 36 45 67 14 11 95 40 63 65 47 70 58 34 65 56 40 70 36 11 95 34 17 47 58 40 58 82 36 89 40 82 19 65 34, 67 40 58 14 65 40 90 36 95 65 34 25 95 47 65 58 36 - 58 40 58, 45 34 59 45 67 11 36 65 65 34, 14 17 95 34 14 63 34 32 82 34 67 95 27 24 40 25 14 65 36 11 36 24 34 25 47 70 25 40 63 27 95 27 “14 65 67 36 65 24 40 65 67 34 11”.

**13 вариант.**

60 46 57 46 52, 28 15 57 39 12 32 60 32 32 46 57 52 55 30 12 61 11 55 57 32 12 41, 37 46 60 37 32 91 52 32 11 55 12 32 75 46 46 57 30 32 20 15 75 46 25 99 20 52 32 52 52 46 67 55 25 55 12 12 32 12 39 52 19 63 “52 99 57 32 36” 75 46 12 61 28 75 99 (18 32 37 57 39 52 99 57 32 36 67 46 60 32 25 63 15 99 91 32 57 25 46 60 46 36 60 19 37 46 57 19 “37 67 99 25 55 12 39 30 25 15 52 46 ” 67 46 20 32 91 12 32). 57 55 37 55 91 55 41 67 57 99 28 75 55. 75 25 55 37 55 60 32 74, 37 57 46 99 57 67 25 99 20 52 55 57 39, 99 20 41 45 52 19 36, 11 12 99 52 52 46 75 25 19 12 19 36, 37 15 67 32 25 55 29 25 46 11 99 52 55 91 99 28 32 37 75 99 36, 60 19 37 46 57 52 19 36. “11 48 99 – 29 25 – 11 60 32 52 55 11 74 55 57 39”, 52 46 60 32 36 18 99 36 37 55 91 46 12 32 57 29 12 32 75 57 25 46 52 52 46 36 25 55 20 60 32 11 75 99, 46 37 52 55 45 32 52 52 19 36 55 67 67 55 25 55 57 15 25 46 36, 78 46 25 11 46 99 91 32 52 15 32 91 46 36 “57 32 63 52 99 75 46 36 11 60 55 11 74 55 57 39 67 32 25 60 46 78 46 60 32 75 55” (63 46 57 41 11 46 75 46 52 74 55 11 60 55 11 74 55 57 46 78 46 37 57 46 12 32 57 99 41, 37 46 78 12 55 37 52 46 63 25 46 52 46 12 46 78 99 99, 46 37 57 55 12 46 37 39 32 45 32 67 41 57 52 55 11 74 55 57 39 37 12 99 18 52 99 91 12 32 57)…

**14 вариант.**

15 48 32 52 32 60 67 32 25 60 19 36 25 55 20 91 55 20 15 25 15 67 25 99 63 46 11 99 12 46 60 78 46 12 46 60 15, 28 57 46 28 99 52, 46 57 60 32 28 55 60 18 99 36 20 55 30 32 20 46 67 55 37 52 46 37 57 39 30 55 20 19, 30 19 12 75 12 55 37 37 99 28 32 37 75 99 91 37 15 63 46 67 15 57 28 99 75 46 91. 60 37 60 46 32 60 25 32 91 41 46 52 67 46 25 55 30 46 57 55 12 52 55 37 46 60 32 37 57 39, 46 30 46 25 15 11 46 60 55 60 37 15 63 46 67 15 57 52 19 32 67 46 11 37 57 15 67 19 75 30 55 20 32 32 91 75 46 37 57 52 19 91 99 11 55 57 28 99 75 55 91 99, 37 99 78 52 55 12 39 52 19 91 99 25 55 75 32 57 55 91 99, 67 25 99 91 55 12 32 36 18 32 91 67 25 99 75 46 37 52 46 60 32 52 99 99 75 57 46 52 61 37 32 52 39 75 46 36 52 99 57 99 60 20 12 32 57 55 60 18 99 91 99 60 52 32 30 32 37 55 37 46 37 60 99 37 57 46 91, 25 55 37 37 19 67 55 41 60 46 25 46 63 55 25 55 20 52 46 74 60 32 57 52 19 63 46 37 12 32 67 99 57 32 12 39 52 19 63 99 37 75 25 - 99 11 55 48 32 67 46 12 46 37 55 91 99 67 25 46 57 99 60 46 67 32 63 46 57 52 19 63 91 99 52. 28 57 46 75 55 37 55 32 57 37 41 67 46 11 37 57 15 67 46 60 60 46 11 52 19 63, 28 99 52 30 19 12 52 32 57 55 75 25 32 57 99 60. 46 11 52 99 57 46 12 39 75 46 37 57 46 12 30 19 37 75 46 12 61 28 75 46 36 99 67 25 32 37 12 46 60 15 57 19 32 “37 67 99 25 55 12 39 75 99” - 75 46 57 46 25 19 32 52 32 20 60 55 52 19 32 78 46 37 57 99, 60 46 57 12 99 28 99 32 46 57 20 11 32 18 52 99 63 67 55 25 57 99 20 55 52, 15 91 32 12 99 67 25 32 46 11 46 12 32 60 55 57 39 30 19 37 57 25 46 99 30 32 20 91 55 12 32 36 18 32 78 46 60 25 32 11 55 11 12 41 37 46 30 37 57 60 32 52 52 46 78 46 46 25 78 55 52 99 20 91 55. 99 60 37 32.

**15 вариант.**

45 74 54 31 10 26 38 23 74, 86 74 54 25 89 26 38 16 74 74 75 16 45 56 90 25 86 90 75 90 10 26 16 74 23 56 86 75 45 16 75 74 95 10 13 31 95 10 51 74 16 89 74, 36 75 95 75 59 36 74 95 74 91 75 31 89 90 23 74 74 90 36 95 89 26 89 90 83 13 26 75 25 86 89 - 75 86 86 75 47 75, 45 86 75 75 16 89 45 74 86 90 74 95 75 25 56 86 75 33, 75 29 95 10 86 89 90 23 89 25 38 90 13 95 74 16 89 74 89 25 26 56 91, 86 75 95 45 10 26 89 90 45 10 19 75 29 74, 33 10 33 31 89 33 89 74 75 29 74 13 38 42 16 83 89 13 29 95 10 13 89 26 89 89, 75 86 86 75 47 75, 45 86 75 36 75 31 90 74 95 16 56 26 25 42 86 56 36 75 46 33 10 46 54 10 16, 25 75 31 89 16 10 33 75 90 83 54 56 25 74 95 31 89 74 54 16 10 36 10 31 10 90 23 89 46 89 16 10 26 74 25 16 56 59 25 90 89 16 38 59, 89 16 10 75 86 26 89 45 16 75 47 75 36 10 95 16 42 25 31 95 56 47 75 47 75 33 75 16 86 89 16 74 16 86 10. 10 90 21 86 75 90 95 74 54 42 86 74, 16 10 29 10 13 74, 51 89 26 89 90 25 90 75 74 56 31 75 90 75 26 38 25 86 90 89 74, 25 36 10 26 89 16 10 45 89 25 86 74 16 38 33 89 91 36 95 75 25 86 83 16 33 10 91 90 33 75 16 31 89 17 89 75 16 89 95 75 90 10 16 16 75 46 36 95 75 91 26 10 31 74, 36 95 89 16 89 54 10 26 89 31 56 23, 51 95 10 26 89 16 10 13 10 90 86 95 10 33 67 95 56 33 86 83, 31 51 74 54 89 29 89 67 23 86 74 33 25 83 90 86 95 89 36 10 26 38 17 10 86 75 26 19 89 16 75 46 - 89 75 33 16 10 86 10 33 56 59 86 16 75 25 90 74 86 89 26 89 25 38, 89 54 56 13 83 33 10 89 47 95 10 26 10, 89 67 56 86 29 75 26 36 75 86 74 26 74 90 89 13 75 95 56…

16 89 45 74 47 75 90 21 86 75 4 6 13 26 75 25 86 89 16 74 29 83 26 75 36 26 75 91 75 47 75, 16 10 75 29 75 95 75 86 - 86 10 33 75 46 16 10 25 86 95 75 46 33 10 33 95 10 13 89 36 95 89 31 10 74 86 29 75 74 90 75 47 75 33 56 95 10 51 10…

10 36 75 86 75 54 36 95 89 23 74 26 33 75 16 74 17 89 36 75 25 86 75 95 75 16 16 89 54 54 83 25 26 42 54 89 29 74 13 31 74 26 38 59. 54 75 95 25 33 75 46 13 54 74 46 16 10 33 75 16 74 17-86 75 36 75 31 10 26 13 16 10 33, 33 75 86 75 95 75 47 75 75 16 89 51 31 10 26 89 45 74 86 90 74 95 75 25 56 86 75 33, 89 21 86 75 29 83 26 75 25 26 75 90 16 75 54 74 31 16 83 46 95 74 90 29 75 74 90 75 46 86 95 56 29 83, 21 86 75 75 13 16 10 45 10 26 75, 45 86 75 16 10 45 10 26 10 25 38 95 10 29 75 86 83, 89 16 89 45 74 47 75 56 51 74 16 74 89 13 54 74 16 89 86 38, 16 74 75 25 86 10 16 75 90 89 86 38, 16 74 36 74 95 74 89 47 95 10 86 38…

**16 вариант.**

15 22 67 30 93 49 22 94 65 94 44 49, 49 39 51 22 75 49 41 11 15 22 49 11 53 51 75 51 78 94, 44 49 27 51 22 67 44 86 51, 26 49 39 51 75 “78 45 94 – 62 75 – 78 11 51 44 49 78 91 49 22 72 14”, 94 11 67 26 93 5 1 44 51 90 67 93 51 44 94 11 67 53 75 67 41 49 45 94 11 49 93 15 30 35 49 15 67 11 67 14, 44 51 45 78 49 11 65 94 14 44 94 86 49 86 94 41 15 20 75 53 75 94 26 67 11, 44 51 53 67 78 67 26 75 51 11 49 11 65 94 14, 35 22 67 51 90 67 15 39 51 75 22 58 53 75 51 27 72 11 49 51 22 15 67 11 15 51 39 44 51 53 67 78 49 93 51 86 88 11 67 27 75 49 26 51 27 51 15 53 93 67 22 44 67 90 67 35 51 75 44 67 90 67 53 75 94 26 75 49 86 49, 44 51 26 44 49 20 18 51 90 67 45 49 93 67 15 22 94.

67 35 51 75 51 78 44 67 14 45 51 15 22 86 67 39 49 44 78 94 75 49 - 94 39 49 26 88 75 15 11 94 86 94 44 90 67 39 94 15 22 75 49 65 94 93 67 14 53 51 75 51 27 51 45 86 49 39 94 78 11 94 44 88 93 94 15 58 11 53 51 75 51 78. 26 78 51 15 58 41 11 49 22 49 93 67 53 75 67 45 51 86 22 67 75 67 11, 36 67 44 49 75 51 14 94 86 75 67 44 65 22 51 14 44 67 11 15 90 94 75 93 30 44 78 49 39 94 93 49 39 53, 44 67 44 51 75 51 49 93 58 44 67 14 26 49 78 49 35 51 14 27 72 93 67 27 72 67 15 11 51 22 94 22 58 11 15 20 27 49 26 88. 67 15 22 49 11 49 93 67 15 58 44 51 39 49 93 67 53 67 93 67 15 94 53 30 22 51 44 22 51 39 44 67 22 72, 86 67 22 67 75 88 20 44 51 26 11 49 44 72 51 90 67 15 22 94 94 15 53 67 93 58 26 67 11 49 93 94 39 49 15 22 51 75 15 86 94. 11 15 51 27 93 94 45 51 86 15 49 39 67 93 51 22 88, 27 93 94 45 51, 27 93 94 45 51, 67 44 11 72 75 49 15 22 49 51 22 44 49 90 93 49 26 49 41, 44 49 11 94 15 49 51 22 44 49 78 90 67 93 67 11 67 14, 88 45 51 53 75 51 86 75 49 15 44 67 15 93 72 65 44 67, 86 49 86 35 49 15 67 11 67 14 67 22 15 86 88 86 94 44 88 78 94 22 53 67 78 44 67 15 44 51 26 44 49 86 67 39 88 20 39 51 93 67 78 94 20, 53 67 15 93 51 78 44 20 20 11 15 11 67 51 14 45 94 26 44 94…

22 94 41 67 44 58 86 67 18 51 93 86 44 88 93 27 51 15 65 88 39 44 72 14 53 94 15 22 67 93 51 22 - 94 39 51 93 67 78 94 30 67 27 67 75 11 49 93 49 15 58, 35 49 15 67 11 67 14 53 67 78 93 67 39 94 93 15 30 11 86 67 93 51 44 86 49 41, 44 67 88 53 49 15 22 58 44 51 88 15 53 51 93, 94 15 11 67 20 49 11 22 67 39 49 22 94 35 51 15 86 88 20 11 94 44 22 67 11 86 88 44 51 11 72 75 67 44 94 93.

78 11 51 22 51 44 94, 27 51 15 65 88 39 44 67 11 72 44 72 75 44 88 11 94 26 -53 67 78 36 20 26 51 93 30 45 49, 53 67 78 41 11 49 22 94 93 94 51 90 67 94 88 11 67 93 67 86 93 94 44 49 78 75 88 90 88 20 15 22 67 75 67 44 88, 11 22 51 39 44 67 22 88.

**17 вариант.**

56 67 92 18 58 39 99 27 87 67 56 25 56 80 67 10 17 92 39 62 25 56 27 24 95 56 31 95 46 27 73 56 31 17 58 39 58 67 95 58 92 56 95 40 24 40 17 92 39 62 69 39 40 17 56 67 58 - 56 18 99 92 46 67 56 87, 69 56 69 39 36 80 17 92 67 27 39 40 87 56 17 58 73 40. 25 56 39 73 56 10 17 92, 56 43 92 80 40 10, 95 56 23 80 40 23 17 40 24 40 25 46 92 69 14 95 67 27 73 95 73 58 87 67 56 73 58. 69 39 58 69 56 95 46 27 23 25 46 92 67 10 17 56 38 58 73 95 92 58 56 38 58 46 73 40 67 92 10. 25 46 92 18 56 46 56 69 92 25 27 17 62 73 56 69 24 80 58 39 62 18 14 17 56 25 46 58 69 58 17 92 95 56 58 87 67 56 43 58 39 73 69 56, 23 17 40 24 40 46 40 24 18 58 23 40 17 92 39 62. 56 80 67 40 95 56 18 17 40 23 56 80 40 46 10 73 58 87 43 58 80 69 27 87 67 58 80 58 17 10 87 73 46 58 67 92 46 56 69 56 95 67 40 87 40 95 58 73 58 92 73 14 39 10 38 58 95 46 40 73 67 56 25 56 69 73 56 46 58 67 67 14 87 67 40 39 73 40 69 17 58 67 92 10 87 92 67 39 73 46 27 95 73 56 46 40 56 67 92 39 56 69 58 46 99 58 67 67 56 73 56 38 67 56 24 67 40 17 92, 24 40 38 58 87 25 46 92 99 17 92. 25 56 67 10 73 92 10 67 58 92 87 58 17 92, 80 17 10 38 58 23 56 95 56 67 95 46 58 73 67 56 25 46 58 80 67 40 24 67 40 38 58 67 14 69 39 58 71 73 92 99 73 27 95 92 - 67 56 56 73 67 92 82 71 73 56 23 56 92 67 58 73 46 58 18 56 69 40 17 56 39 62.

67 58 25 46 56 99 17 56 92 87 92 67 27 73 14, 95 40 95 56 67 27 69 92 80 58 17 51 58 17 62 92 82 67 58 17 58 23 95 56 23 56 92 71 95 24 56 73 92 38 58 39 95 56 23 56 25 27 73 58 99 58 39 73 69 92 10 - 73 46 92 25 27 17 62 73 40 25 56 25 46 40 69 56 87 27 18 56 46 73 27, 27 39 14 25 40 67 67 14 58 38 58 46 73 56 69 56 31 27 31 87 56 31 73 27 87 18 17 58 46 56 69, 17 40 87 25 56 38 58 95, 25 58 46 58 95 17 36 38 40 73 58 17 58 31 92 95 67 56 25 56 95. 73 46 92 69 14 25 27 95 17 14 82 71 95 46 40 67 40 69 69 92 80 58 69 58 46 73 92 95 40 17 62 67 14 82 25 46 10 87 56 27 23 56 17 62 67 92 95 56 69 - 56 67 92 39 40 87 14 58, 67 92 95 40 95 56 31 56 99 92 18 95 92…

18 56 80 46 56 39 73 92 46 40 80 92, 56 67 25 56 69 73 56 46 92 17 25 46 56 39 58 18 10 25 56 17 36 18 92 69 99 27 36 39 10 51 92 73 40 73 27: “38 73 56 56 80 92 67 38 58 17 56 69 58 95 25 56 39 73 46 56 92 17, 80 46 27 23 56 31 24 40 69 39 58 23 80 40 46 40 24 17 56 87 40 73 62 39 87 56 43 58 73”. 92, 25 56 82 17 56 25 40 69 25 56 25 17 58 38 27 39 73 46 40 99 92 17 27 69 24 67 40 95 73 56 23 56, 38 73 56 67 40 25 40 46 67 92 95 80 56 17 43 58 67 18 80 92 73 58 17 62 67 56 39 73 56 10 73 62 67 40 99 27 82 58 46 58, 80 56 39 73 40 17 95 92 67 43 40 17 92 24 25 46 92 99 92 73 14 82 67 40 80 95 56 17 58 67 56 87 67 56 43 58 67.

**18 вариант.**

67 58 26 19 88 23 32 37 15 23 90 63 71 46 63 26-63 26 58 24 63 23 37 32 95 67 63 15 32 88 58 26 - 67 26 58 67 41 16 24 90 63 52 30 24 49 63 26 88 26 37 23 38 23 16 67 58 23 90 26 41 90 63 68 24 58 58 26 76 85 15 67 76 24 15 24. 19 26 15 23 38 88 26 63 15 32 88 58 24 24 90 88 24 16 23 63 71 63 23 37, 46 63 26 41 54 37 15 23 95 67 67 58 24 38 23 76 24 63 67 16 67 68 26 68 90 24, 67 58 23 46 24 37 63 26 – 63 26 58 24 19 16 32 85 54 44 26 46 24 58 71 41 54 90 63 15 26 90 88 24 16 23 24 63 90 26 26 63 68 24 63 90 63 68 32 11 30 67 24 68 54 68 26 88 54 67 24 30 24, 46 24 19 26 88 26 41 15 26 19 26, 85 15 67 76 24 63 90 52 37 16 24 68 24 63 23 63 71, 68 15 23 95 67 58 23 67 88 24 26 16 26 19 67 46 24 90 37 23 52, 85 32 90 63 71 88 23 95 24 32 58 24 19 26 67 58 24 41 32 88 24 63 88 26 37 23 38 23 63 24 16 71 90 63 68, 58 26 37 46 24 76 32 58 23 76 16 67 83 58 52 52 37 16 24 68 24 63 23? 63 26-63 26… 49 63 26 63 56 67 58 23 16 85 26 38 68 26 16 52 16 26 88 58 67 76 76 23 73 26 76 15 24 83 67 63 71 58 24 90 37 26 16 71 37 26 38 23 88 23 46. 58 24 41 54 16 26 58 67 37 23 37 26 44 37 15 23 95 67, 90 26 68 24 15 83 24 58 58 26 44 73 68 23 63 37 67 76 67 63 15 24 58 67 15 26 68 23 58 58 54 76 67 15 24 41 52 63 23 76 67 - 85 15 26 90 63 26-58 23 85 15 26 90 63 26 26 37 15 24 90 63 58 54 24 85 23 15 63 67 38 23 58 54, 88 23 68 58 54 76-88 23 68 58 26 19 15 26 38 67 68 83 67 24 88 26 41 15 23 63 71 90 52 68 90 24 95 24 88 26 26 85 16 26 63 23 67 76 85 24 15 67 23 16 67 38 76 23, 90 67 15 24 46 71 88 23 58 58 26 44 41 23 38 54, 90 68 26 11 32 19 15 26 38 32 68 37 26 58 29 24 37 26 58 29 26 68 68 54 85 26 16 58 67 16 67. 58 23 19 15 52 58 32 16 67 58 26 46 58 26 44 85 26 15 26 44, 85 26 15 24 38 23 16 67 37 26 16 11 46 37 32, 85 15 26 58 67 37 16 67 58 23 41 23 38 32 85 26 88 85 26 37 15 26 68 26 76 76 15 23 37 23, 38 23 16 26 95 67 16 67 90 85 26 16 88 11 95 67 58 54 76 67 58, 85 26 90 63 15 24 16 52 16 67 67 38 19 15 23 58 23 63 26 76 24 63 26 68 67, 90 85 15 23 68 24 88 16 67 68 26 15 24 83 67 68, 46 63 26 88 26 90 63 23 63 26 46 58 26 58 23 85 23 37 26 90 63 67 16 67, 38 16 26 15 23 88 58 26 85 26 16 11 41 26 68 23 16 67 90 71 88 24 16 26 76 15 32 37 90 68 26 67 73 67 32 41 15 23 16 67 90 71 68 26 90 68 26 52 90 67 41 24 38 76 23 16 24 44 83 24 19 26 88 16 52 90 24 41 52 32 15 26 58 23.

**19 вариант.**

34 92 45 25 90 30 25 71 16 62 37 71 55 71 89 18 96 62 55 85 22 71 11 62 62 24 62 89 71 55 55 62 85 55 16 71 92 71 24 55 62 11 62 - 90 30 49 30 24 55 18 71 24 16 85 92 30 55 18 71 52 37 85 55 24 18, 49 30 92 62 22 25 30 22 85 24 16 18 73 92 58 89 30 67 71 25, 90 58 89 55 30 20 86 71 16 25 30 24 16 45 89 85 25 62 14 49 30 24 16 18 - 89 92 62 52 20 11 71 68 16 62 49 62 96 62 37 71 55 62, 25 62 96 85 62 55 30 34 24 16 92 30 96 85 71 46 92 62 52 62 14, 49 30 92 30 89 30 55 62 25 25 62 55 24 71 92 34 62 34, 49 62 22 30 16 18 94 39 96 30 25 62 55 24 62 89 71 90 90 30 92 30 37 85 34 30 45 86 85 14 85 34 62 52 58 16 30 89 96 71 16 25 30 14 85, 24 16 30 92 18 94 25 62 14 49 30 24, 62 89 67 30 92 49 30 55 55 18 94 39 62 55 30 92 85 25 85 49 92 62 22 30 20 52 92 71 89 71 52 71 55 19, 85 90 62 89 96 85 22 30 34 67 30 20 34 52 37 62 55 71 24 16 19 45 -25 30 25 -71 11 62-16 30 14 52 62 24 16 30 16 62 22 55 62 62 49 18 16 55 62 11 62 49 58 16 71 67 71 24 16 34 71 55 55 85 25 30, 14 30 16 92 62 24 30 24 55 71 14 30 96 18 14 24 16 30 37 71 14, 34 62 52 85 55 49 92 71 25 92 30 24 55 18 94 52 71 55 19 92 71 67 85 34 67 71 11 62 49 62 85 24 25 30 16 19 24 22 30 24 16 19 20 55 30 89 71 92 71 11 58. 49 92 71 52 71 96 19 55 62 24 25 92 62 14 55 18 71 49 62 37 85 16 25 85, 55 71 24 49 62 24 62 89 55 18 71 49 92 85 34 96 71 22 19 34 55 85 14 30 55 85 71 24 71 92 19 71 90 55 18 73 11 92 30 89 85 16 71 96 71 94.

85 14 71 96 62 24 19 85 62 92 58 37 85 71, 30 25 30 25 37 71. 49 92 85 96 85 22 55 18 73 92 30 90 14 71 92 62 34 62 73 62 16 55 85 22 85 94 55 62 37, 34 16 62 92 62 94, 25 30 92 14 30 55 55 18 94 67 34 71 94 46 30 92 24 25 85 94 49 71 92 62 22 85 55 55 85 25 24 52 34 58 14 20 52 71 24 20 16 25 30 14 85 49 92 85 22 85 55 52 30 96 62 34, 30 16 30 25 37 71 49 62 16 71 92 16 18 94 49 85 24 16 62 96 71 16-25 62 96 19 16 89 62 96 71 71 22 71 14 52 34 30 52 46 30 16 85 96 71 16 55 71 11 62 34 62 90 92 30 24 16 30, 55 62 58 73 62 37 71 55 55 18 94 85 24 14 30 90 30 55 55 18 94 - 85 14 71 55 55 62 16 30 25 62 71 62 92 58 37 85 71 14 62 37 55 62 89 71 90 62 24 62 89 18 73 49 92 62 89 96 71 14 49 92 85 62 89 92 71 24 1685 34 49 62 92 16 62 34 18 73 16 92 58 86 62 89 30 73. 34 24 71 49 92 62 52 58 14 30 55 62. 90 52 71 67 55 85 71 49 62 96 85 46 30 85 24 89 62 96 19 67 85 14 49 62 52 62 90 92 71 55 85 71 14 62 16 55 62 24 20 16 24 20 25 24 58 89 10 71 25 16 30 14 24 30 34 16 62 14 30 16 85 22 71 24 25 85 14 62 92 58 37 85 71 14 55 30 49 96 71 22 71, 90 30 16 62 55 71 62 24 62 89 62 55 30 34 62 92 62 22 71 55 55 18 94 25 30 92 30 89 85 55 85 96 85 49 92 62 24 16 71 55 19 25 85 94 49 85 24 16 62 96 71 16 34 25 30 92 14 30 55 71 34 90 52 71 67 55 85 73 14 71 24 16 30 73 24 22 85 16 30 45 16 24 20 55 71 49 92 71 14 71 55 55 18 14 30 16 92 85 89 58 16 62 14 58 34 30 37 30 45 86 71 11 62 24 71 89 20 25 30 89 30 96 19 71 92 62, 49 85 24 19 14 71 55 55 62 11 62 92 30 90 92 71 67 71 55 85 20 55 71 16 92 71 89 58 45 16 85, 34 62 89 86 71 14, 49 62 52 62 90 92 71 55 85 94 55 71 34 18 90 18 34 30 45 16, 49 62 25 30 24 85 73 49 62 14 62 86 19 45 55 71 24 62 16 34 62 92 20 16 22 71 11 62-16 62 55 71 90 30 25 62 55 55 62 11 62.

**20 вариант.**

16 74 53 74 47 47 85 31 85 66 74 29 58 55 74 16 96 74 66 85 55 11 66 58 96 11 12 91 74 74 50 96 11 12 91 85 49 53 58 85 47 11 33 74 26 74 31 23 29 47 85 26 45 29 85 55 74 29, 96 11 12 33 85 96 74 29, 33 11 96 74 28 58 29 74 12 96 11 47 55 11 - 66 85 68 28 74 29 35 53 28 58 47 35 16 85 96 47 74 29 96 85 33 85 91 91 23 85, 47 29 85 96 28 11 21 18 58 85 91 74 29 85 91 61 28 58 33 66 11 28 74 33, 66 85 68 28 74 29 35 53 28 58 29 96 85 33 85 91 88 35 55 61 66 58 91 85 29 55 74 96 74 49 33 58 96 74 29 74 49, 47 55 11 96 85 91 61 28 58 85 11 29 55 74 50 35 47 23, 68 96 74 33 11 31 91 23 85 68 96 35 12 74 29 58 28 58-55 96 11 28 58, 91 85 29 85 47 55 61 74 55 28 35 31 11 29 12 43 29 53 11 43 47 43 58 91 85 29 85 31 74 33 74 28 35 31 11 47 16 85 53 58 29 53 11 43 16 74 79 11 96 91 11 43 33 11 53 58 91 11… 31 74 29 74 66 61 91 74 47 28 74 96 74 74 91 74 55 33 85 55 58 66, 88 55 74 47 96 85 31 58 29 47 85 68 74 38 55 74 68 74 96 11 12 91 74 74 50 96 11 12 58 43 91 85 16 74 16 11 31 11 85 55 47 43 91 58 29 74 85 91 91 23 26, 91 58 16 74 66 58 45 85 49 47 28 58 26 33 11 53 58 91, 29 74 74 50 18 85 29 74 28 96 85 47 55 91 74 47 55 43 26, 91 11 47 28 74 66 61 28 74 33 74 79 91 74 47 35 31 58 55 61 16 74 55 74 33 35, 88 55 74 74 91 29 58 31 85 66 47 29 85 96 26 74 55 35 96 23, 91 85 91 11 50 66 21 31 11 85 55 47 43 91 58 33 11 66 85 49 53 58 26 16 96 58 12 91 11 28 74 29 88 96 85 12 29 23 88 11 49 18 58 91 23, 28 11 28-55 74: 33 74 50 58 66 61 91 23 26 16 11 55 96 35 66 85 49, 16 74 47 55 74 29 91 11 74 50 74 88 58 91 85, 16 96 74 29 85 96 28 58 31 74 28 35 33 85 91 55 74 29, 12 11 47 55 11 29, 50 66 74 28 16 74 47 55 74 29… 91 58 88 85 68 74 16 74 31 74 50 91 74 68 74. 47 58 85 45 85 91 91 74 85 91 11 50 66 21 31 85 91 58 85 91 85 91 11 53 35 55 28 35 16 96 58 50 11 29 66 43 66 74 74 16 55 58 33 58 12 33 11.

74 91 16 74 47 33 74 55 96 85 66 66 85 29 85 85 - 55 11 33 74 55 16 11 91 11 33 85 96 58 28 11 91 23 74 55 26 74 31 58 66 11 11 47 62 11 66 61 55 58 96 74 29 11 91 91 11 43 31 74 96 74 68 11, 91 85 29 16 96 58 33 85 96 35 79 85, 31 11 66 85 28 74 91 85 55 11 28 11 43 74 79 58 29 66 85 91 91 11 43. 58 35 55 23 28 11 66 11 47 61 74 91 11 16 96 43 33 85 26 74 91 61 28 74 29 55 74 55 47 11 33 23 49 68 74 96 74 31 74 28, 68 31 85 58 26 53 85 47 55 85 96 28 11 31 74 66 79 91 11 50 23 66 11 29 23 49 55 58 91 11 33 85 47 55 91 74 68 74 91 85 66 85 68 11 66 11.

**21 вариант.**

40 77 40, 29 75 58 75 28 75! 15 61 75 23 40 52 67 29 29 54 52 11 15 75 65 58 54 15 84 40 29 54 61 67 28 75 77 75 58 84 11 18 77 75 61 67 28 54 35 40, 77 52 11 15 75 37 11 84 11 52 54 28 11, 28 40 28 11 29 49 37 75 35 75 13, 35 29 40 52 84 40 58 28 75 13 35 54 84 15 54 65 28 75 13 15 75 37 58 40 13 11 28 58 11 29 75 90 29 49 72 40 11 58 37 80 15 18 72 35 40 29 84 11 13 11 28 15 11 84 29 75 41 13 54 84 75 29 75 41, 54 15 75 52 11 11 37 58 29 75 61 75 13 37 61 75 82 11 28 40 15 54 84 40 13 54 52 35 40 54 90 29 75 29 37 11 18 82 37 58 40 84 54 28 28 49 46 80 52 11 84, 35 40 35 54 13 54 15 40 61 54 61 54 61 11 58 90 40 37 58 75 52 75 15 75 80 29 61 11 28 54 80 28 40 35 75 28 29 11 41 11 84 11 58 40 35 54 46 29 75 58 58 84 11 46 52 20 41 13 75 29 75 35 - 37 20 84 84 11 40 61 54 37 58 54 65 11 37 35 75 11 37 75 65 11 58 40 28 54 11, 11 37 61 54 29 52 18 13 40 58 67 37 80, 28 75 13 11 37 58 28 49 46, 28 40 52 75 15 75 61 40 77 40 58 67, 29 15 75 61 28 11 18 37 58 84 40 54 29 40 11 58. 54 33 75 28 40 77 61 80 52 28 75 15 75 35 40 90 49 29 40 11 58 52 75 33 61 11 37 58 67, 15 84 75 80 29 61 11 28 28 18 20 54 46 52 11 84 82 40 29 75 41 29 15 11 84 29 18 20 13 54 84 75 29 18 20: 28 18 35 40 35 82 11, 75 28 40 75 58 15 84 40 29 54 61 40 28 40 11 29 84 75 15 11 41 37 35 54 41 92 84 75 28 58 26 11 61 49 41 37 58 84 11 61 35 75 29 49 41 33 40 58 40 61 67 75 28 54 58 75 84 82 11 37 58 29 11 28 28 75 15 75 84 29 40 61 40 75 58 28 75 72 11 28 54 80 37 77 11 84 13 40 28 37 35 75 41 54 13 15 11 84 54 11 41, 40 29 52 75 33 40 29 75 35 75 52 18 29 72 11 37 58 28 40 52 26 40 58 75 13 33 11 84 11 77 75 29 49 11 33 40 58 40 84 11 54 75 52 28 75 77 75 54 90 29 75 11 28 28 49 46 15 75 84 58 75 29 26 11 61 49 46 52 29 40 65 40 37 40 15 40 61 54 61 54 15 75 58 75 41 58 75 65 35 11 18 77 75 84 54 90 75 28 58 40, 77 52 11 35 40 35 75 13 18 -58 75 33 52 54 58 11 61 67 28 75 13 18 29 75 80 35 11 15 75 65 18 52 54 61 37 80 77 11 84 13 40 28 37 35 54 41 35 84 11 41 37 11 84… 75 33 19 11 35 58 54 29 28 75 37 58 54 84 40 52 54 37 58 75 54 58 18 58 75 65 28 54 58 67, 65 58 75 29 75 29 58 75 84 18 20 13 54 84 75 29 18 20 90 52 11 72 28 54 41, 15 18 37 58 67 54 28 11 29 11 61 54 35 54 41 29 75 11 28 28 75-13 75 84 37 35 75 41 92 61 75 58 29 13 11 37 58 11 37 37 75 20 90 28 54 35 40 13 54 15 40 58 84 18 61 54 84 75 29 40 61 15 84 54 61 11 77 40 20 23 54 11 29 75 52 49 54 15 40 84 18 84 40 90 29 84 75 52 11 33 49 52 40 82 11 37 58 84 11 61 80 61 15 75 28 40 37 58 75 80 23 54 13, 40 28 11 15 84 54 29 54 52 11 29 72 54 13 37 80 15 75 52 29 75 52 28 49 13 61 75 52 35 40 13 35 84 54 77 37-13 40 84 54 28 11.

**22 вариант.**

56 96 31 57 87 37 56 75 84 77 87 24 96 73 68 75, 56 75 50 37 16 42 68 77, 77 20 73 37 37 49 56 77 39 77 87 37, 39 73 37 12 84 96 16 91 64 56 91 87 37. 75 56 84 73 16 91 68 94 75 75 31 57 87 75 44 16 37 84 73 57 75 56 96 49 77 73 96 14 87 75 12 57: 96 84 87 75 56 77 44 37 28 37 68 37 56 56 75 68 96 56 96 73 56 75 50 37 16 42 68 77, 56 75 84 77 87 24 96 73 68 75, 96 84 87 75 73 77 26 73 37 87 41 68 37 84 77 87 24 96 73 68 77 31 96 49 50 37 16 42 68 77 75 87 75 50 37 16 42 37 68 31 96 49 84 77 87 24 96 73 68 75 - 56 96 73 37 39 73 37 56 96 12 64 37 28 75 73 41, 56 37 28 77 35 96 56 96 44 16 75 31 87 75 35 77 73 41 84 61. 12 84 96 44 16 96 35 56 75 96 16 77 84 68 87 77 28 57 87 96 73 61 73 68 39 96 16 73 91, 12 35 75 49 56 41 84 87 96 28 91 96 73 56 96 26 96 28 87 96 56 56 37 44 16 96 73 12 37 16 61 73 41 49 77 44 77 84 56 37 14 12 77 16 75 77 56 73. 56 91 35 56 37 68 77 68 26 37 35 56 37 31 57 84 73 16 96 96 37 73 84 82 28 77 84 26 77 73 57 12 77 73 41 84 61, 91 31 75 16 77 73 41 84 61 68 39 96 16 73 37 12 37 14 26 77 73 96 16 75 75 49 50 37 16 37 28 68 77, 12 84 73 91 44 77 96 73 12 84 75 87 91 49 77 44 77 84 56 37 14 12 77 16 75 77 56 73 37 73 64 37 28 77…

12 96 84 41 37 68 16 91 35 77 82 22 75 14 26 75 16 12 56 96 49 77 44 56 37 84 73 77 87 56 96 44 16 37 84 73 37 39 91 35 75 26 - 12 16 77 35 28 96 31 56 57 26. 44 37 28 37 49 16 96 12 77 73 41 84 87 96 28 37 12 77 87 37 12 84 96 64 75 12 84 61. 44 41 82 22 75 64 44 75 12 37 84 37 87 28 77 73 75 68 37 12 - 12 73 37 26, 39 73 37 37 56 75 56 96 84 37 87 28 77 73 75 68 75 12 37 12 84 96, 77 50 16 91 44 44 77 49 77 64 12 77 73 77 75 49 12 37 96 56 56 37 14 68 37 56 73 16 16 77 49 12 96 28 68 75, 44 16 96 84 73 77 16 96 87 37 50 37 50 37 84 73 75 56 75 39 56 37 50 37 64 26 57 16 61 - 12 73 37 26, 39 73 37 37 56 12 37 12 84 96 56 96 44 37 16 73 41 96 75 87 75 12 87 77 28 96 87 96 94, 75 87 75 73 37 75 28 16 91 50 37 96 12 37 28 56 37 26 87 75 94 96, 77 44 37 87 68 37 12 56 75 68 49 28 96 42 56 96 14 73 77 14 56 37 14 44 37 87 75 94 75 75. 12 84 96 12 37 49 26 37 35 56 37, 68 37 50 28 77 91 84 87 37 12 87 96 56 56 37 50 37 84 75 50 56 77 87 77 56 96 73 56 77 91 84 87 37 12 87 96 56 56 37 26 26 96 84 73 96.

**23 вариант.**

22 10 75 62 47 10 74 10 24 88 47 39 35 66 15 75 58 10 47 64 53 53 85 66 35 10 69 62 28 10 24 53 66 49 53 47 47 10 49 64 10 58 39 28 22 88 17 10 79 47 88 15 47 66 22 53. 44 47 10 85 17 10 28 53 24 75 44 35 51 66 75 58 53 47 53 64 88. 35 10 35 72 62 28 10 24 66 47 88 17 10 69, 44 66 80 37 80 10 24 69 49 88 75 39 37 74 53 17 66 58 28 66 17 88 47 53 88 53 85 66 35 66 15, 22 37 28 75 58 28 10, 35 66 58 66 17 62 88 53 75 85 62 58 62 28 10 88 79 39, 66 35 10 69 10 28 79 53 75 39 28 49 10 28 47 66 69 47 10 35 66 74 62 42 74 88 75 58 10 42. 79 53 17 66 35 53 88 28 66 17 66 58 10 72 62 24 53 17 10 75 85 10 42 47 37 58 62, 37 75 10 49 39 72 10 37 58 66 47 37 24 10 28 75 37 74 88 17 35 10 42. 44 28 66 79 88 24 28 42 66 24 24, 51 49 88 58 37 74 10 47 47 62 88 69 88 17 35 10 24 10 69 62 72 35 66 66 58 17 10 31 10 24 53 64 28 88 58 62 53 49 88 58 10 24 53 53 47 58 88 17 39 88 17 10. 37 49 53 28 53 58 88 24 39 47 66, 47 66 42 66 69 44 53 47 47 88 37 69 47 10 24 74 88 47 44. 66 47 85 17 66 58 44 47 37 24 17 88 51 53 75 58 17 10 64 53 66 47 47 37 97 35 47 53 51 37. 44 28 69 44 24 17 37 22 35 37, 66 72 7 41 03 54 73 7 24 85 88 17 66 28 72 17 66 47 69 66 28 37 97 22 88 17 47 53 24 39 47 53 64 37 53, 75 35 24 66 47 53 28 79 53 75 39 47 10 49 17 10 75 35 17 62 58 62 74 53 75 58 17 10 47 53 64 10 74 53, 75 58 66 24 35 47 37 24 75 44 75 85 88 17 28 66 15 53 69 74 47 66 31 88 75 58 28 10 47 88 66 31 53 49 10 47 47 66 75 58 88 15, 35 66 58 66 17 62 88 85 66 49 75 58 88 17 88 51 10 24 53 74 88 47 44 25 58 66 15 47 66 22 39 97. 74 66 88 53 74 44, 42 66 17 42 88 24 37 53 75 72 66 17 42 88 75, 72 62 24 66 47 10 22 88 17 58 10 47 66 28 35 47 53 51 88, 53 22 88 17 47 53 24 10 88 80 88 47 88 37 75 85 88 24 53 28 62 75 66 42 47 37 58 39.

**24 вариант.**

61 52 16 36 26 14 54 16 45 24 29 45 95 11 29 36 95 86 36 16 29 45 14 52 49 75 36 47 97 36 93 95 61 54 26 61 97 36 26 86 45 97 49 95 41 29 11 47. 93 49 30 61 86 95 11 93 56 11 86 83 89 95 36 47 49 16 95 11 37 36 93 14 54 26 61 95 11 30 86 36 16 36 47 21 86 11 33 49, 26 36 29 95 11 47 14 95 11 30 95 45 86 16 49 95 95 14 89 93 30 36 16 14 29, 33 11 54 29 14 89 14 71 11 52 16 36 19 49 95 95 83 89, 36 52 95 49 26 49 95 95 83 89 52 11 54 98 26 86 16 11 93 36 89; 75 93 49, 29 11 29 97 36 47 95 14 54 36 26 41 47 95 49, 26 86 36 61 54 11 97 54 61 33 95 11 61 26 29 11 47 49 89 29 11. 21 86 36 52 83 54 11 26 11 47 11 61 52 36 54 41 19 11 61 29 36 47 95 11 86 11 30 75 36 26 86 14 95 14 56 49. 61 86 36 54 29 95 45 54 93 30 49 16 41, 36 95 11 97 36 93 93 11 54 11 26 41. 97 36 93 97 36 86 36 54 29 36 47 75 36 16 49 54 11 54 98 26 86 16 11. 30 49 49 52 49 71 33 11 54 36 26 86 95 36 47 26 30 49 86 49 61 45 71 95 11 54 26 49 52 61. 95 11 45 71 29 36 89 33 49 54 49 71 95 36 89 29 16 36 30 11 86 14 54 49 33 11 54 61, 97 36 26 86 11 16 49 30 19 14 89 14 36 52 16 98 71 75 19 14 89, 14 16 11 71 75 54 61 93 83 30 11 54 54 49 97 95 14 95 45 95 11 97 36 86 36 54 29 49. 61 45 26 54 83 19 11 54 75 36 54 36 26. 95 49 26 36 30 26 49 47 47 36 89 - 52 49 71 36 52 49 16 86 36 95 36 30, 95 49 97 16 14 61 86 95 83 89, 97 36 37 36 33 14 89 95 11 47 11 75 95 14 86 36 78 36 95 95 45 98 71 11 97 14 26 41.

- 45 93 14 30 14 86 49 54 41 95 36, - 26 29 11 71 11 54 36 95, - 95 11 26 93 30 36 49 14 47 83 36 93 95 36. 30 97 16 36 24 49 47, 30 36 26 95 49 95 14 24 86 36 95 49 26 97 36 26 36 52 95 36 30 83 71 30 11 86 41 45 93 14 30 54 49 95 14 49. 61 16 36 52 29 36 26 97 16 36 26 14 54:

- 71 95 11 24 14 86, 30 26 49 21 86 36 26 36 95?

- 97 16 14 24 49 47 97 36 26 54 49 93 95 14 89 26 36 95. - 33 49 26 86 36 47 36 95 97 36 29 11 71 11 54 95 11 97 45 26 86 36 89 97 45 71 83 16 49 29,

26 86 36 61 30 19 14 89 95 11 47 16 11 47 36 16 95 36 89 29 16 83 19 29 49 95 36 24 95 36 75 36 26 86 36 54 14 29 11. - 86 49 52 49 97 16 14 93 49 86 26 61, 95 11 30 49 16 95 36 49, 45 30 14 93 49 86 41 47 95 36 33 49 26 86 30 36 26 95 36 30, 97 16 49 33 93 49 24 49 47 93 36 52 49 16 49 19 41 26 61 93 36 21 86 36 89 95 36 24 14. 29 11 29 36 49 26 49 75 36 93 95 61 24 14 26 54 36 97 36 86 30 36 49 47 45 29 11 54 49 95 93 11 16 98?

**25 вариант.**

48 84 13 33 94 13 48 42 33 46 82, 84 13 82 48 94 82 46 84 33 42 13 88 82 84 16 46 16 25 82 50 17 48 13 42 61 37 78 50 51 16 82 42 13 82 84 16 46 16 50 48 17 34 13 76 82 25 82 16 72 82 46 48 69 17 82 28 82, 28 84 48 51 75 48 75 84 33 46 16 46 33 84 33 17, 75 33 37 82 13 17 34 16 38 48 37 17 16 46 33. 82 17 13 58 94 25 33 69 58 13 33 46 76 82 75 48 46 33 17 16 34, 16 34 76 82 25 33 69 58 13 33 46 48 50 51 13 94 48, 38 42 82 17 16 48 94 42 78 13 50 16 37 48. 13 76 37 16 28 82 37 64 17 48 17 48 17 33 13 16 94 42 17 82 28 82 72 58 46 82 94 82 72 37 33 17 82 13 94 48, 38 42 82 84 82 13 48 46 82 94 78 76 82 13 16 84 33 42 78 51 75 48 51 94 82 76 64 16 50 16 38 42 82 69 37 34 42 17 58 17 48 69 84 37 33 13 94 42 13 51 61 21 16 48: 28 82 37 82 84 33, 75 33 37 25 16 48 16 88 82 46 82 84 17 58 48 94 42 37 33 17 58, 94 82 25 37 82 13 16 21 33, 94 25 37 58 42 58 48 13 69 48 50 17 58 88 28 46 51 72 16 17 33 88, 72 82 37 82 69 84 34 21 16 48 50 82 37 34 25 82 37 33 72 46 16, 82 37 51 84 16 34 13 82 91 17 58, 16 17 94 42 37 51 50 48 17 42 58 13 37 33 38 48 13 33 17 16 34 16 50 51 69 58 25 16, 76 46 48 17 16 42 48 46 78 17 58 88 75 48 17 21 16 17, 17 48 76 82 84 13 16 75 17 58 48 69 13 48 69 84 58 16 76 46 33 17 48 42 58, 25 37 33 94 25 16, 25 82 42 82 37 58 50 16 76 82 46 78 69 51 61 42 94 34 17 48 13 48 37 17 58 48, 25 82 28 84 33 76 16 64 51 42 94 13 82 16 50 48 37 69 25 16 48

25 33 37 42 16 17 58, 37 33 94 42 48 17 16 34 16 50 16 17 48 37 334 65 8 94 82 13 94 48 50 16 16 88 94 82 25 37 82 13 48 17 17 58 50 16 69 33 50 48 38 33 42 48 46 78 17 58 50 16 94 13 82 91 94 42 13 33 50 16, 94 48 37 48 72 37 34 17 58 88 33 17 28 48 46 82 13, 38 48 91 88 46 48 72 - 88 13 33 46 33 16 76 37 48 13 82 69 17 48 94 48 17 16 48 28 82 94 76 82 84 33, 37 33 69 84 33 38 51 17 33 28 37 33 84 13 64 25 82 46 33 88, 19 16 28 51 37 58 76 42 16 98 16 98 33 37 48 91, 88 37 33 17 34 21 16 48 94 34 13 94 33 50 82 50 94 48 37 84 98 48 76 16 37 33 50 16 84, 42 48 17 78 72 58 25 33, 17 33 25 82 42 82 37 82 50 76 82 25 82 16 42 94 34 69 48 50 46 34, 16 37 58 72 58, 17 33 25 82 42 82 37 82 91 94 42 82 16 42

72 58 25, 76 51 94 42 58 17 16 13 94 48 50 16 46 82 94 42 16 13 82 28 82 72 82 28 33. 82 17 51 13 16 84 48 46 13 48 21 16 17 48 82 76 16 94 51 48 50 58 48, 42 33 25 16 48, 25 33 25 51 46 16 98 58, 82 94 13 48 21 48 17 17 58 48 28 33 69 82 13 58 50 16 37 82 75 25 33 50 16, 16 25 16 42 33, 25 82 42 82 37 58 91 51 50 16 37 33 48 42 76 37 16 69 13 51 25 33 88 38 48 46 82 13 48 38 48 94 25 82 28 82 28 82 46 82 94 33.

# ПРИЛОЖЕНИЕ 2

Варианты заданий по теме: «Нахождение НОД»

|  |  |  |
| --- | --- | --- |
| **№**  **вар-та** | **а** | **b** |
| **1** | 6390 | 5571 |
| **2** | 9276 | 9878 |
| **3** | 9270 | 5313 |
| **4** | 1826 | 5563 |
| **5** | 4688 | 436 |
| **6** | 8224 | 5584 |
| **7** | 4420 | 5550 |
| **8** | 5730 | 7341 |
| **9** | 3927 | 2366 |
| **10** | 8064 | 7544 |
| **11** | 2037 | 5460 |
| **12** | 8464 | 138 |
| **13** | 4710 | 3306 |
| **14** | 2074 | 7412 |
| **15** | 4925 | 2200 |
| **16** | 3952 | 9328 |
| **17** | 3837 | 6222 |
| **18** | 9156 | 3858 |
| **19** | 6138 | 8308 |
| **20** | 4479 | 7567 |
| **21** | 6992 | 4200 |
| **22** | 9740 | 5604 |
| **23** | 6054 | 8658 |
| **24** | 6966 | 5328 |
| **25** | 4756 | 7975 |
| **26** | 1836 | 4536 |
| **27** | 4896 | 7016 |
| **28** | 300 | 4092 |
| **29** | 3073 | 8925 |
| **30** | 4727 | 2745 |
| **31** | 6735 | 8285 |
| **32** | 5852 | 8250 |

# ПРИЛОЖЕНИЕ 3

Варианты заданий по теме: «Решение уравнений с двумя неизвестными»

1). 5852х+8250у=44;

2). 8285х-6735у=10;

3). 4727х+2745у=5;

4). 8925х+3073у=14;

5). 4092х+300у=24;

6). 4896х+7016у=16;

7). 4536х+1836у=216;

8). 7975х+4756у=58;

9). 6966х+5328у=36;

10). 8658х+6054у=18;

11). 5604х+9740у=12;

12). 4200х+6992у=16;

13). 7567х+4479у=2;

14). 6222х+3837у=9;

15). 3858х+9156у=12;

16). 6138х+8308у=62;

17). 3952х+9328у=32;

18). 2200х+4925у=50;

19). 2074х+7412у=34;

20). 3306х+4710у=12;

21). 138х+8464у=92;

22).5460х+2037у=63;

23). 7544х+8064у=8;

24). 3927х+2366у=14;

25). 7341х+5730у=6;

26). 5550х+4420у=20;

27). 5584х+8224у=32;

28). 436х+4688у=28;

29). 5563х+1826у=16;

30). 9270х+5313у=9;

31). 9276х+9878у=56;

32). 6390х+5571у=27.

# ПРИЛОЖЕНИЕ 4

Варианты заданий по теме: «Нахождение остатков от деления чисел»

|  |  |  |
| --- | --- | --- |
| **1** вариант | а) 19131 на 6; | б) 1197 на 13; |
| **2** вариант | а) 31151 на 14; | б) 6619 на 7; |
| **3** вариант | а) 2318 на 18; | б) 6219 на 7; |
| **4** вариант | а) 383169 на 45; | б) 5226 на 17; |
| **5** вариант | а) 109345 на 14; | б) 2449 на 13; |
| **6** вариант | а) 243402 на 1000; | б) 7422 на 11; |
| **7** вариант | а) 2757 на 8; | б) 48248 на 5; |
| **8** вариант | а) 12371 на 9; | б) 182424 на 7; |
| **9** вариант | а) 8297 на 3; | б) 25282 на 11; |
| **10** вариант | а) 1587 на 4; | б) 21146 на 13; |
| **11** вариант | а) 2749 на 10; | б) 4164 на 17; |
| **12** вариант | а) 13291 на 9; | б) 22881 на 23; |
| **13** вариант | а) 7422 на 12; | б) 2185 на 19; |
| **14** вариант | а) 5226 на 15; | б) 38401 на 41; |
| **15** вариант | а) 1197 на 22; | б) 21199 на 19; |
| **16** вариант | а) 6719 на 6; | б) 3367 на 37; |
| **17** вариант | а) 31254 на 42; | б) 10768 на 7; |
| **18** вариант | а) 2549 на 12; | б) 281440 на 31; |
| **19** вариант | а) 23265 на 12; | б) 91156 на 43; |
| **20** вариант | а) 15259 на 8; | б) 18726 на 5; |
| **21** вариант | а) 14453 на 5; | б) 30589 на 29; |
| **22** вариант | а) 8999 на 9; | б) 12102 на 11; |
| **23** вариант | а) 5447 на 25; | б) 15134 на 13; |
| **24** вариант | а) 7844 на 22; | б) 16257 на 3; |
| **25** вариант | а) 8256 на 6; | б) 24265 на 23. |

# ПРИЛОЖЕНИЕ 5

Варианты заданий по теме: «Решение сравнений»

|  |  |
| --- | --- |
| **1** вариант | 11х ≡ 7 (mod 13) |
| **2** вариант | 82х ≡ 26 (mod 30) |
| **3** вариант | 16х ≡ 2 (mod 14) |
| **4** вариант | 132х ≡ 9 (mod 35) |
| **5** вариант | 14х ≡ 3 (mod 5) |
| **6** вариант | 5х ≡ 7 (mod 11) |
| **7** вариант | 23х ≡ 9 (mod 12) |
| **8** вариант | 8х ≡ 5 (mod 9) |
| **9** вариант | 7х ≡ 3 (mod 22) |
| **10** вариант | 8х ≡ 6 (mod 13) |
| **11** вариант | 19х ≡ 5 (mod 6) |
| **12** вариант | 31х ≡ 12 (mod 14) |
| **13** вариант | 24х ≡ 1 (mod 11) |
| **14** вариант | 101х ≡ 5 (mod 17) |
| **15** вариант | 7х ≡ 24 (mod 43) |
| **16** вариант | 6х ≡ 32 (mod 37) |
| **17** вариант | 9х ≡ 6 (mod 23) |
| **18** вариант | 10х ≡ 12 (mod 19) |
| **19** вариант | 15х ≡ 23 (mod 31) |
| **20** вариант | 20х ≡ 32 (mod 41) |
| **21** вариант | 12х ≡ 19 (mod 29) |
| **22** вариант | 21х ≡ 35 (mod 40) |
| **23** вариант | 13х ≡ 42 (mod 56) |
| **24** вариант | 17х ≡ 2 (mod 35) |
| **25** вариант | 10х ≡ 3 (mod 33) |