

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**Федеральное государственное автономное образовательное учреждение  
высшего образования**  
**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**  
**Невинномысский технологический институт (филиал)**

**Методические указания по выполнению лабораторных работ  
по дисциплине**  
**«Персональная кибербезопасность»**

Направление подготовки	15.03.04 Автоматизация технологических процессов и производств
Направленность (профиль)	Информационно-управляющие системы
Квалификация выпускника	бакалавр
Форма обучения	Очная
Учебный план	2022 года

Ставрополь, 2022

УДК 004.94  
УДК 004.67  
ББК 16.8  
К 755  
С 172

Печатается по решению  
Учебно-методического совета  
Северо-Кавказского федерального  
университета

**Персональная кибербезопасность:** Методические указания по выполнению лабораторных работ / Ю.Н. Кочеров, Д. В. Самойленко – Ставрополь: Изд-во СКФУ, 2022. – 138 с.

Методические указания по выполнению лабораторных работ подготовлены в соответствии с программой дисциплины «Персональная кибербезопасность», разработанной в соответствии с требованиями ФГОС ВО по направлению подготовки бакалавров 15.03.04 Автоматизация технологических процессов и производств. В лабораторном практикуме последовательно изложены базовые принципы защиты персональной информации, описаны математические модели криптографических алгоритмов и численные методы их реализации в соответствии с темой каждой работы, составлен перечень контрольных вопросов, а также список рекомендуемой литературы.

**Рецензенты:**

А.А. Евдокимов, канд. техн. наук, доцент, доцент кафедры информационных систем, электропривода и автоматики Невинномысского технологического института (филиала) СКФУ;

Д.В. Гринченков канд. техн. наук, доцент, декан факультета информационных технологий и управления, заведующий кафедрой «Программное обеспечение вычислительной техники» ФГБОУ ВО «ЮРГПУ (НПИ) имени М.И. Платова».

УДК 004.94  
УДК 004.67  
ББК 16.8  
К 755  
С 172

© ФГАОУ ВО «Северо-Кавказский  
федеральный университет», 2022  
© Кочеров Ю.Н. 2022  
© Самойленко Д.В. 2022

## СОДЕРЖАНИЕ

Введение.....	5
Тема 4. Методы защиты информации с применением симметричных алгоритмов шифрования	
Лабораторная работа №1 «Изучение математических моделей шифра простой замены» .....	6
Тема 4. Методы защиты информации с применением симметричных алгоритмов шифрования	
Лабораторная работа №2 «Изучение математических моделей шифра Виженера и численных методов его реализации» .....	33
Тема 4. Методы защиты информации с применением симметричных алгоритмов шифрования	
Лабораторная работа №3 «Изучение математической модели симметричного алгоритма шифрования на примере XOR и численного метода его реализации» .....	87
Тема 5. Методы защиты информации с применением асимметричных алгоритмов шифрования	
Лабораторная работа №4 «Изучение математической модели асимметричного алгоритма шифрования и численного метода его реализации на примере алгоритма RSA».....	99
Тема 6. Методы защиты информации с применением методов основанных на разделении данных	
Лабораторная работа №5 «Изучение математических моделей схем порогового разделение данных, основанных на геометрических законах и численных методов их реализации» .....	109
Тема 6. Методы защиты информации с применением методов основанных на разделении данных	
Лабораторная работа №6 «Изучение математических моделей схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации» .....	126
Приложение А – Таблица частот биграмм русского языка .....	136
Приложение Б – Таблица ASCII кодов .....	137
Пример в приложении В – Форма титульного листа .....	138

## Введение

В связи с тем, что объем киберугроз с каждым годом все больше растет то вопросы кибербезопасность, становятся все более актуальными.

При изучении курса студент сможет познакомиться с основными математическими моделями защиты информации и изучить численные методы их реализации.

Целью изучения дисциплины является формирование компетенций будущего бакалавра по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств, а также дать студентам общее представление о безопасности в информационном обществе, сформировать понимание технологий достижения информационной безопасности во всех сферах деятельности и освоить системный подход для решения поставленных задач в области кибербезопасности.

Задачи изучения дисциплины заключаются в:

- приобретении студентами знаний и практических навыков в области, определяемой основной целью дисциплины;
- приобретении необходимых навыков, позволяющих изучить на практике принципы работы методов защиты информации.

Дисциплина Персональная кибербезопасность направлена на формирование компетенций, определенных ФГОС ВО обучающихся в процессе выполнения работ.

Последовательность лабораторных работ соответствует логической структуре их прохождения. Предлагаемые методические указания содержат материал, который рекомендуется использовать студентам при выполнении лабораторных работ.

## Тема 4. Методы защиты информации с применением симметричных алгоритмов шифрования

### Лабораторная работа №1 «Изучение математических моделей шифра простой замены»

**Цель работы:** изучить принципы и математическую модель шифра простой замены.

#### Программа работы

- 1) Изучить теоретический материал, математические и алгоритмические особенности шифра простой замены.
- 2) В соответствии с заданием расшифровать текст, закодированный шифром простой замены.

#### Элементы теории

Криптоанализ шифра простой замены основан на использовании статистических закономерностей языка. Так, например, известно, что в русском языке частоты букв распределены следующим образом (Таблица 1.1). Гистограмма распределения частот букв представлена на рисунке 1.1.

Таблица 1.1 – Частоты букв русского языка (в 32-буквенном алфавите со знаком пробела)

Буква	Ранг буквы	Частотность	Буква	Ранг буквы	Частотность
–	1	0,175	Я	17	0,018
О	2	0,09	Ы	18	0,016
Е, Ё	3	0,072	З	19	0,016
А	4	0,062	Ь, Ы	20	0,014
И	5	0,062	Б	21	0,014
Т	6	0,053	Г	22	0,013
Н	7	0,053	Ч	23	0,012
С	8	0,045	Й	24	0,01
Р	9	0,04	Х	25	0,009
В	10	0,038	Ж	26	0,007
Л	11	0,035	Ю	27	0,006
К	12	0,028	Ш	28	0,006
М	13	0,026	Ц	29	0,004
Д	14	0,025	Щ	30	0,003
П	15	0,023	Э	31	0,003

У	16	0,021	Ф	32	0,002
---	----	-------	---	----	-------

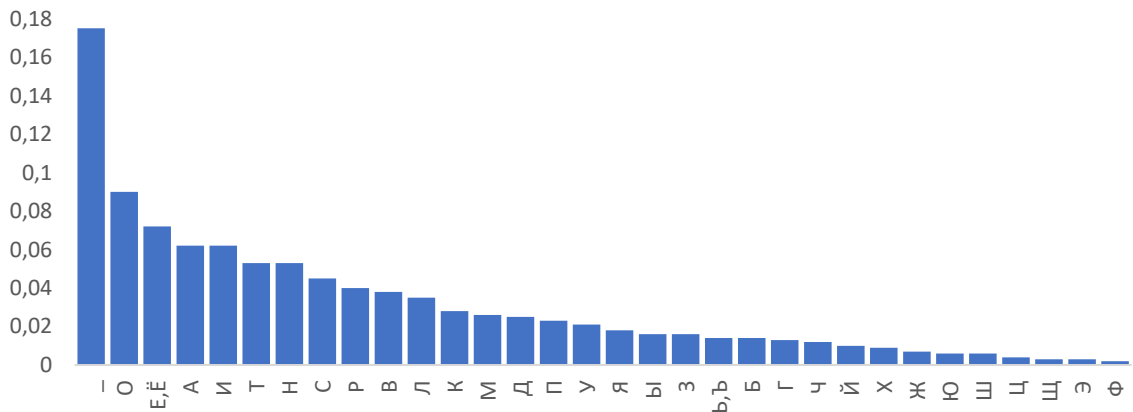


Рисунок 1.1 – Гистограмма распределения частот русского языка

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;

Полезной является информация о сочетаемости букв, то есть о предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм.

Имеется в виду таблица, в которой слева и справа от каждой буквы расположены наиболее предпочтительные "соседи" (в порядке убывания частоты соответствующих биграмм) (Приложение А). В таких таблицах обычно указывается также доля гласных и согласных букв (в процентах), предшествующих (или следующих за) данной буквой.

### Пример криптоанализа шифра простой замены

Рассмотрим пример анализа шифра простой замены. Известно, что при шифровании каждая буква заменена на двухзначное число, все знаки

препинания сохранены, а слова разделены несколькими пробелами. Частоты букв русского языка приведены в таблице 1.1.

Рассмотрим следующее сообщение:

47 39 42 27 27 50 48 38 43 42 43 28 45 51 25 46 47 45 39 45 27 34 25 45 31  
 44 36 28 43 42 43 34 42 27 42 36 46 31 42 32 42 22 43 50 25 50 47 , 50 22 42  
 31 34 47 42 41 35 46 37 47 36 46 23 27 46 45 27 42 21 50 25 45 36 50 52 27 50  
 45 44 38 43 25 50 48 38 43 47 50 43 45 51 36 50 21 45 27 45 25 42 43 50 25 50  
 47 , 42 43 42 22 24 45 33 45 43 50 39 50 47 46 37 47 34 40 50 25 42 . 51 25  
 46 47 45 39 45 27 34 25 45 31 44 36 28 43 42 43 34 26 22 38 51 45 25 46 33 45  
 27 43 42 36 28 27 50 21 50 46 38 38 36 45 39 50 47 42 27 46 23 31 42 47 46 38  
 46 33 50 38 43 46 26 32 32 45 22 43 46 47 27 50 38 43 46 43 45 51 36 50 21 45  
 27 45 25 42 43 50 25 50 47 50 43 25 42 40 50 52 45 48 33 50 35 27 50 38 43 46  
 21 50 25 45 36 50 52 27 34 37 44 38 43 25 50 48 38 43 47 . 25 42 31 25 42 40 50  
 43 42 27 34 25 45 22 50 33 45 27 39 42 30 46 46 51 25 46 47 34 40 50 25 45  
 43 45 51 36 50 21 45 27 45 25 42 43 50 25 42 46 21 50 25 45 36 50 52 27 50 21  
 50 44 38 43 25 50 48 38 43 47 42 .

Подсчитаем частоты шифрообразований (Таблица 1.2). Гистограмма частот шифрообразований представлена на рисунке 1.2.

Таблица 1.2 – Частоты шифрообразований

Число	Частота	Число	Частота	Число	Частота	Число	Частота	Число	Частота
50	40	46	20	51	7	48	5	23	2
45	31	47	17	22	6	28	4	26	2
43	28	38	14	31	6	40	4	35	2
42	27	36	12	39	6	52	4	24	1
25	25	34	9	33	5	32	3	30	1
27	20	21	8	44	5	37	3	41	1

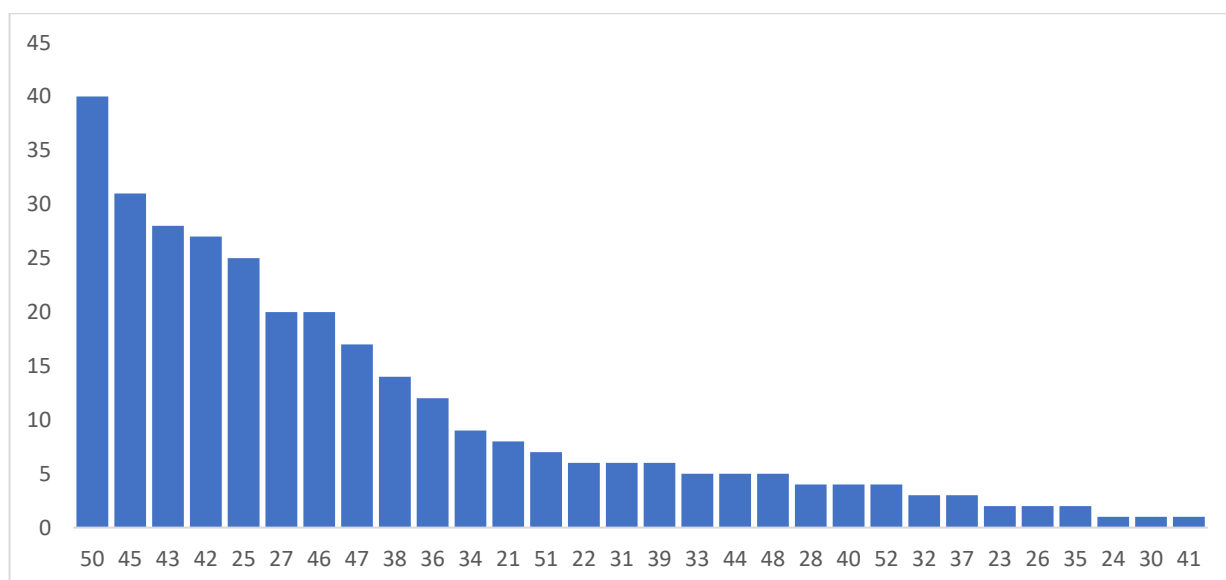


Рисунок 1.2 – Гистограмма частот шифрообразований

Из таблицы 1.1 и гистограммы (рисунок 1.1) видно, что чаще всего встречается буква «О», а за ней буква «Е». Из таблицы 1.2 и гистограммы (рисунок 1.2) видно, что чаще всего встречается значение «50» (40 раз), на следующем месте значение «45» (31 раз). Из этого можно выдвинуть гипотезу что числу «50» соответствует буква «О», а числу «45» соответствует буква «Е».

В связи с тем, что размерность текста не велика то закономерности русского языка проявляются не обязательно в строгом соответствии с таблицей биграмм (Приложение А). Тем не менее можно выявить некоторые закономерности. Например зная, что числу «45» соответствует буква «О» то в шифротексте можно выделить такую комбинацию как: «45 39 45» воспользовавшись таблицей биграмм можно сделать вывод что число «39» это буква «Д».

На следующем этапе можно воспользоваться частым сочетанием: «50 47» воспользовавшись таблицей биграмм и вышеупомянутыми заключениями можно сделать вывод что число «47» это буква «В».

Зная, что «39» это значение буквы «Д», а в нашем тексте она сочетается либо с буквой «О», либо с числом «42» то воспользовавшись таблице биграмм можно сделать вывод что число «42» это буква «А».



Далее рассмотрим число «27» видно, что оно часто сочетается с «О» более того в тексте присутствует сочетание «27 27» воспользовавшись таблицей биграмм можно сделать вывод что «27» это буква «Н».

Заменяя в шифротексте все предложенные буквы видно, что буква «О» часто сочетается с числом «38», также есть сочетание «38 38» зная какие буквы были однозначно определены и воспользовавшись таблицей биграмм можно сделать вывод что число «38» это буква «С».

Теперь видно, что буква «С» часто сочетается с числом «43», тогда из таблицы биграмм видно, что «С» чаще всего сочетается с буквой «Т» следовательно «43» это буква «Т».

Выполнив все предложенные замены, можно увидеть, что первые два слова приставляют собой «в данно48 стат28е» тогда «48» это буква «Й», а «28» буква «Ь».

Далее видно, что буква «О» часто сочетается с числом «25» тогда воспользовавшись приложением А можно сделать вывод что число «25» это буква «Р».

Видно, что присутствует сочетание «\_46\_» тогда вероятнее всего что число «46» это союз, следовательно, зная предыдущие замены можно сделать заключение что «46» это буква «И».

Количество сочетаний в оставшемся тексте буквы «Н» и числа «34» составляет 4 раза. Тогда из биграмм видно, что числу «34» соответствует буква «Ы».

После всех замен видно, что в тексте два раза присутствует следующее сочетание «51риведены» следовательно число «51» соответствует букве «П». Также присутствуют сочетания «вы40ора» и «вы40оре» из которых можно сделать вывод что число «40» это буква «Б».

Из оставшихся сочетаний: «44стройство»; «44стройств»; «44стройства» можно выдвинуть гипотезу что числу «44» соответствует буква «У».

Проанализировав оставшийся текст, выделяется следующая сточка «в данной статье приведены результаты» из которой видно, что числу «31» соответствует буква «У», а числу 36 соответствует буква «Л».

Из сочетаний: «вли23ние» и «исследовани23» видно, что числу «23» соответствует буква «Я».

Из оставшегося текста «в данной статье приведены результаты анализа 32а22торов, о22азыва4135и37 влияние на 21орело52ное устройство тепло21енераторов, а та2224е 33етодов и37 выбора. приведены результаты 2622спери33ентально21о исследование зависи33ости 263232е22тивности тепло21енераторов от рабо52ей 33о35ности 21орело52ны37 устройств. разработаны ре22о33енда30ии при выборе тепло21енератора и21орело52но21о устройства.» видно что числу «32» соответствует буква «Ф», числу «22» соответствует буква «К», числу «21» соответствует «Г».

Тогда из сочетаний: «горело52ное»; «рабо52ей»; «горело52ного», видно, что число «52» это «Ч».

Из оставшегося текста «в данной статье приведены результаты анализа факторов, оказыва4135и37 влияние на горелочное устройство теплогенераторов, а так24е 33етодов и37 выбора. приведены результаты 26кспери33ентального исследование зависи33ости 26ффективностм теплогенераторов от рабочей 33о35ности горелочны37 устройств. разработаны реко33енда30ии при выборе теплогенератора и горелочного устройства.» видно что цифре «33» соответствует буква «М», «24» буква «Ж», «37» буква «Х», «35» буква «Щ», «41» буква «Ю», а «30» буква «Ц».

Проведя оставшиеся замены получим текст «в данной статье приведены результаты анализа факторов, оказывающих влияние на горелочное устройство теплогенераторов, а также методов их выбора. приведены результаты экспериментального исследование зависимости эффективности теплогенераторов от рабочей мощности горелочных устройств. разработаны рекомендации при выборе теплогенератора и горелочного устройства.».

Гистограмма частот букв в дешифруемом тексте представлена на рисунке 1.3.

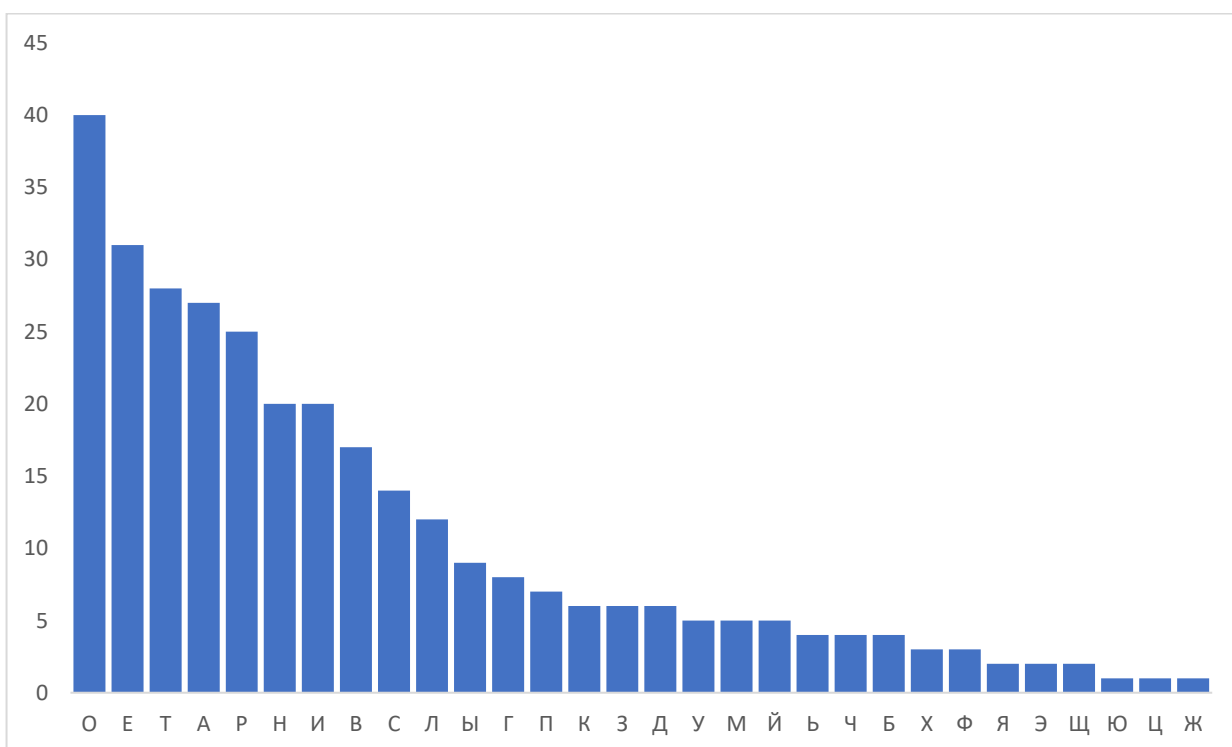


Рисунок 1.3 – Гистограмма частот букв в дешифруемом тексте

### **Указания по технике безопасности**

В начале каждого семестра, со студентами должен проводиться инструктаж по технике безопасности в лаборатории. Во время нахождения студента в лаборатории и выполнения лабораторных работ студент не должен нарушать инструкции по охране труда с персональным компьютером ИОТ-37-ИВЛ-19, и инструкцию о мерах пожарной безопасности ИБП-01-2016.

### **Методические указания к выполнению работы**

Каждому студенту необходимо расшифровать закодированный текст в соответствии с вариантом (таблица 1.2)

При выполнении работы разрешается использовать любые технические и программные средства.

Таблица 1.3 – Задания для студента по вариантам

Вариант	Задание
1)	<p>36 25 38 38 25 28 52 22 25 22 26 28 35 23 52 37 28 46 43 38 25 25 38  25 48 47 51 40 22 39 43 31 23 37 25 38 47 34 35 23 37 32 31 23 39 40  49 23 38 22 25 24 38 32 33 21 39 25 38 23 37 36 48 28 37 23 51 37 43  36 43 38 47 28 37 32 52 23 22 38 32 33 51 36 25 38 47 34 . 52 22 39  23 47 22 43 48 26 38 25 28 23 22 39 25 52 48 26 47 41 39 25 43 22 37  25 24 38 40 29 39 23 48 26 37 39 25 51 37 47 22 47 47 38 25 30 47  47 . 52 39 25 51 37 47 22 47 43 49 35 43 39 43 36 23 37 32 33 22 43  33 38 23 48 23 41 47 34 47 39 25 52 22 40 46 47 49 47 52 35 23 48 26  51 23 37 25 38 47 43 49 22 43 33 38 47 21 47 35 39 47 52 22 39 23 47  22 43 48 26 52 22 37 43 21 39 40 35 38 32 33 52 22 39 23 47 22 43 48  26 38 32 33 23 31 27 43 21 22 23 37 , 47 38 24 43 38 43 39 40 - 52 22  39 23 47 22 43 48 29 52 22 25 48 23 38 43 23 31 33 23 36 47 49 23 31  32 22 26 51 38 25 21 23 49 32 49 52 35 39 23 43 21 22 47 39 23 37 25  38 47 43 49 47 35 39 47 49 43 38 43 38 47 43 49 39 25 51 48 47 44 38  32 33 35 25 39 25 49 43 22 39 23 37 , 21 23 22 23 39 32 43 47 52 35  23 48 26 51 40 29 22 52 28 37 52 23 37 39 43 49 43 38 38 23 49 52 22  39 23 47 22 43 48 26 52 22 37 43 . 38 25 21 39 40 35 38 23 49 35 39  23 43 21 22 43 40 35 23 36 39 28 36 44 47 21 25 49 23 24 43 22 31  32 22 26 25 52 52 23 39 22 47 49 43 38 22 39 25 51 48 47 44 38 32 33  21 39 25 38 23 37 36 48 28 39 25 51 38 32 33 30 43 48 43 34 . 35 23  41 39 40 51 23 44 38 23 - 39 25 51 41 39 40 51 23 44 38 32 43 39 25 31  23 22 32 - 37 25 24 38 25 28 44 25 52 22 26 35 39 23 30 43 52 52 25  36 23 52 22 25 37 21 47 52 22 39 23 47 22 43 48 26 38 32 33 35 39 23  43 21 22 23 37 , 25 21 39 25 38 32 - 38 25 47 31 23 48 43 43 37 25  24 38 32 43 39 43 52 40 39 52 32 , 47 52 35 23 48 26 51 40 43 49 32 43  36 48 28 36 23 52 22 47 24 43 38 47 28 42 22 23 34 30 43 48 47 , 23</p>

	52 23 31 43 38 38 23 38 25 52 22 39 23 47 22 43 48 26 38 23 34 35 48 23 46 25 36 21 43 .
2)	23 45 21 48 50 47 26 23 34 25 40 21 45 40 24 40 40 47 21 38 33 43 26 43 29 25 23 25 43 46 47 50 34 43 28 47 23 25 45 38 35 23 47 46 35 51 43 35 23 . 50 26 40 50 47 40 35 50 47 26 40 23 47 46 32 37 50 47 25 43 47 43 28 23 33 40 52 22 46 28 47 40 25 25 40 29 26 43 50 47 43 46 47 23 28 40 32 23 49 46 50 47 25 40 52 43 50 50 46 31 45 40 25 , 51 40 50 47 26 40 46 45 45 38 33 45 46 45 43 21 32 46 42 43 30 23 35 40 52 26 43 29 40 35 . 51 26 23 49 23 45 40 31 47 40 35 48 35 40 42 46 47 52 38 47 37 23 50 51 40 32 37 29 40 25 43 45 23 46 50 47 26 40 23 47 46 32 37 45 38 33 35 43 47 46 26 23 43 32 40 25 45 23 29 28 40 24 40 28 43 49 46 50 47 25 43 23 50 40 28 26 43 30 46 45 23 46 23 33 40 52 22 46 35 40 25 , 25 38 51 40 32 45 46 45 23 46 26 43 52 40 47 45 46 28 25 43 32 23 36 23 41 23 26 40 25 43 45 45 38 35 23 50 40 47 26 48 21 45 23 28 43 35 23 , 40 47 50 47 48 51 32 46 45 23 46 23 50 51 40 32 45 23 47 46 32 34 40 47 51 26 40 46 28 47 43 , 51 26 46 50 32 46 21 48 34 50 25 40 23 32 23 49 45 38 46 41 46 32 23 , 45 43 26 48 44 46 45 23 46 47 26 46 52 40 25 43 45 23 31 45 40 26 35 43 47 23 25 45 40 - 47 46 33 45 23 49 46 50 28 23 33 21 40 28 48 35 46 45 47 40 25 23 29 - 29 43 50 42 43 47 38 33 50 26 40 28 40 25 25 38 51 40 32 45 46 45 23 34 51 26 40 46 28 47 43 . 27 47 23 36 43 28 47 40 26 38 40 52 48 50 32 43 25 32 23 25 43 39 47 25 40 29 26 43 50 47 43 45 23 46 45 46 40 52 33 40 21 23 35 40 50 47 23 25 51 26 40 25 46 21 46 45 23 23 50 47 26 40 23 47 46 32 37 45 40 - 47 46 33 45 23 49 46 50 28 40 31 27 28 50 51 46 26 47 23 29 38 .
3)	50 43 51 44 45 21 30 38 44 41 38 41 52 33 33 38 24 43 41 21 44 45 38 29 51 31 21 41 43 41 38 52 24 45 44 45 35 41 24 41 31 44 51 44 41 48 21 50 43 29 51 44 38 21 45 31 35 45 27 44 45 43 45 30 23 24 45 36 29 41 46 50 43 45 48 22 41 21 45 48 41 31 29 38 30 45 48 41 44 50

	<p>43 41 43 46 42 41 45 44 51 30 23 44 45 48 50 29 38 40 38 . 41 44 40 38  24 50 28 52 24 45 44 45 35 41 24 41 31 44 51 44 41 48 41 41 44 50  43 41 43 46 42 41 45 44 51 30 23 44 45 25 45 29 38 27 41 35 51 , 29 51  50 50 22 41 43 51 44 44 28 38 36 45 35 38 43 45 40 41 24 38 21 50 38  35 41 29 44 45 25 45 32 51 44 24 51 , 45 36 29 38 40 38 30 49 37 43 25  45 43 45 21 44 45 50 43 23 50 43 29 51 44 28 24 40 51 30 23 44 38 48  39 38 35 46 29 51 31 21 41 43 41 37 . 36 45 40 51 44 44 28 35 29 38  48 43 41 44 25 51 29 45 50 50 41 49 36 45 24 51 31 28 21 51 38 43 36  29 45 32 30 38 35 44 46 37 41 44 50 43 41 43 46 42 41 45 44 51 30 23 44  46 37 50 45 50 43 51 21 30 49 37 34 46 37 . 21 50 43 51 43 23 38 41  50 50 30 38 40 46 37 43 50 49 45 50 44 45 21 44 28 38 41 44 50 43 41  43 46 42 41 45 44 51 30 23 44 28 38 36 29 45 32 30 38 35 28 , 36 29 38  25 29 51 40 28 , 51 41 35 38 44 44 45 41 44 50 43 41 43 46 42 41 45  44 51 30 23 44 28 38 30 45 21 46 39 24 41 - 36 29 38 36 49 43 50 43  21 46 37 34 41 38 29 51 31 21 41 43 41 37 52 24 45 44 45 35 41 24 41  31 44 51 44 41 48 , 21 28 49 50 44 38 44 28 41 26 35 38 26 51 44 41  31 35 28 41 36 45 50 30 38 40 50 43 21 41 49 40 30 49 29 45 50 50  41 48 50 24 45 48 52 24 45 44 45 35 41 24 41 , 36 29 38 40 30 51 25 51  37 43 50 49 50 36 45 50 45 32 28 21 28 26 45 40 51 41 31 44 41 26 .</p>
4)	<p>30 32 44 37 44 41 46 23 37 32 32 26 37 44 23 48 30 37 35 44 32 50 30  38 29 23 38 32 31 , 38 44 23 37 52 37 35 49 48 46 32 33 49 39 38 32 44  41 44 46 45 39 38 40 38 34 48 48 48 39 51 38 23 26 37 27 48 38 39 39  38 34 38 26 38 43 46 40 48 23 38 30 37 39 48 50 , 37 44 37 47 52 46  38 32 39 38 30 39 31 46 36 44 37 29 31 23 37 28 30 48 44 48 50 . 29  38 43 25 46 23 47 48 30 37 46 44 32 50 , 25 44 38 48 32 29 38 40 41 28  38 30 37 39 48 46 30 47 37 25 46 32 44 30 46 38 27 46 39 47 48 36  51 51 46 47 44 48 30 39 38 32 44 48 30 39 46 43 23 46 39 48 50 48 23  46 37 40 48 28 37 27 48 48 48 39 51 38 23 26 37 27 48 38 39 39 38 34 38  26 38 43 46 40 48 23 38 30 37 39 48 50 30 38 23 34 37 39 48 28 37 27</p>

	<p>48 50 45 29 38 47 37 28 37 44 46 40 50 38 44 43 37 25 48 39 37 30  40 38 52 46 39 39 31 24 47 37 29 48 44 37 40 39 46 32 38 30 32 46 26  47 38 23 23 46 47 44 39 38 , 44 37 47 47 37 47 39 46 33 25 48 44 31  30 37 46 44 26 39 38 52 46 32 44 30 38 51 37 47 44 38 23 38 30 . 29  23 46 43 40 37 34 37 46 44 32 50 48 32 29 38 40 41 28 38 30 37 44 41  29 38 47 37 28 37 44 46 40 48 23 37 32 25 46 44 37 47 38 26 26 46 23  25 46 32 47 38 24 36 51 51 46 47 44 48 30 39 38 32 44 48 , 29 23 48 26  46 39 50 46 26 31 46 29 23 48 33 29 23 37 30 40 46 39 48 48 48 39 30  46 32 44 48 27 48 38 39 39 38 - 32 44 23 38 48 44 46 40 41 39 31 26 48  29 23 38 46 47 44 37 26 48 . 29 23 48 30 38 43 50 44 32 50 38 32 39 38  30 39 31 46 51 37 47 44 38 23 31 , 30 40 48 50 35 49 48 46 39 37 38  27 46 39 47 33 36 47 38 39 38 26 48 25 46 32 47 38 24 36 51 51 46 47  44 48 30 39 38 32 44 48 30 39 46 43 23 46 39 48 50 44 46 45 39 38 40  38 34 48 48 48 39 51 38 23 26 37 27 48 38 39 39 38 34 38 26 38 43 46  40 48 23 38 30 37 39 48 50 30 29 23 38 46 47 44 39 38 - 32 44 23 38 48  44 46 40 41 39 31 45 38 23 34 37 39 48 28 37 27 48 50 45 .</p>
5)	<p>22 26 38 46 34 33 39 27 30 27 22 31 25 27 34 29 50 38 24 38 26 33 39  38 50 25 27 50 27 41 27 45 38 51 37 30 38 39 43 38 37 37 33 45 24  . 37 27 39 27 26 33 51 38 37 31 23 22 38 26 38 37 25 27 33 25 37 44  50 33 26 33 43 33 50 50 52 39 , 23 38 25 44 38 37 25 26 38 37 25 38  31 25 45 38 22 26 38 37 21 40 33 39 50 38 24 38 34 33 25 . 41 27  35 25 38 45 26 33 39 44 , 30 27 30 22 38 30 27 41 52 45 27 33 25 37  25 27 25 31 37 25 31 30 27 , 22 26 38 31 41 38 43 34 38 38 32 33 50 29  39 50 38 24 38 27 45 27 26 31 48 31 22 38 45 26 33 40 51 33 50 31 48  25 26 27 50 37 22 38 26 25 50 52 23 37 26 33 51 37 25 45 . 46 38 34 29  43 27 44 50 27 24 26 21 41 30 27 50 27 51 38 26 38 40 50 38 33 22  38 34 38 25 50 38 22 26 31 45 38 51 31 25 30 46 52 37 25 26 38 39 21  31 41 50 38 37 21 27 37 49 27 34 29 25 38 45 38 24 38 22 38 30 26 52  25 31 44 , 45 26 33 41 21 34 29 25 27 25 33 22 38 32 25 31 30 27 40</p>

	<p>51 52 48 24 38 51 41 27 45 38 51 37 30 38 39 21 43 38 37 37 33 25  26 33 46 21 33 25 37 44 26 33 39 38 50 25 . 50 27 24 26 21 41 30 27 50  27 43 38 37 37 33 33 36 33 21 45 33 34 31 32 31 25 37 44 , 30 38 24  51 27 46 21 51 33 25 22 38 37 25 26 38 33 50 21 32 27 37 25 38 30 51  38 26 38 24 31 , 37 45 44 41 52 45 27 47 36 31 48 50 38 45 52 48 30  31 26 38 45 37 30 31 48 39 38 37 25 37 41 27 45 38 51 37 30 31 39 43  38 37 37 33 . 27 45 25 38 39 38 46 31 34 29 50 27 44 51 38 26 38 24 27  45 24 . 37 27 39 27 26 33 22 38 41 27 45 38 51 37 30 38 39 21 43 38  37 37 33 50 21 40 51 27 33 25 37 44 45 30 27 22 31 25 27 34 29 50 38  39 26 33 39 38 50 25 33 21 40 33 50 33 22 33 26 45 52 48 24 38 51  , 38 51 50 27 30 38 26 27 46 38 25 27 25 27 30 31 50 33 50 27 32  31 50 27 33 25 37 44 , 27 30 27 40 51 21 47 45 33 37 50 21 45 37 33  46 38 34 33 33 21 23 21 51 43 27 33 25 37 44 33 33 37 38 37 25 38 44  50 31 33 . 45 38 22 26 38 37 38 37 25 27 33 25 37 44 27 30 25 21 27  34 29 50 52 39 31 50 27 37 33 24 38 51 50 44 43 50 31 48 51 33 50  29 .</p>
6)	<p>27 45 41 30 38 33 31 39 24 41 28 46 45 41 40 51 24 21 33 31 33 46 29  27 33 49 36 49 40 31 35 49 49 38 29 38 33 31 39 31 37 41 33 29 28 31  28 31 29 38 28 29 39 41 40 31 27 29 24 28 49 33 41 24 41 52 49 40 30  45 29 37 24 41 28 29 32 29 37 41 33 29 28 31 . 38 27 29 36 29 25 21  26 36 31 33 41 36 31 33 49 43 41 38 48 29 32 29 49 28 31 33 51 45 28  29 32 29 36 29 30 41 24 49 45 29 39 31 28 49 42 27 29 30 29 37 45 31  28 38 29 38 33 31 39 45 31 38 44 49 45 42 26 25 41 52 30 29 37 31 39  48 49 38 51 24 21 47 29 31 24 24 26 36 49 28 31 33 28 29 32 29 33 49  27 31 , 51 38 33 31 28 29 39 24 41 28 29 29 27 33 49 36 31 24 21 28 29  41 27 45 29 35 41 28 33 28 29 41 38 29 29 33 28 29 44 41 28 49 41 48  29 36 27 29 28 41 28 33 29 39 36 29 30 49 47 49 35 49 45 29 39 31 28 28  29 32 29 35 41 36 41 28 33 31 , 33 45 41 37 51 41 36 29 41 30 24 42  27 29 24 51 43 41 28 49 42 36 31 33 41 45 49 31 24 31 38 51 24 51 43</p>



	<p>44 41 28 28 46 36 49 22 48 38 27 24 51 31 33 31 35 49 29 28 28 46 36 49  38 39 29 52 38 33 39 31 36 49 , 27 29 24 51 43 41 28 46 36 31 33 41 36  31 33 49 43 41 38 48 49 41 36 29 30 41 24 49 38 33 45 29 49 33 41 24  21 28 29 - 33 41 34 28 49 43 41 38 48 49 34 38 39 29 52 38 33 39 37 41  33 29 28 31 49 48 49 28 41 33 49 48 31 49 34 49 40 36 41 28 41 28  49 42 38 51 43 41 33 29 36 39 45 41 36 41 28 28 29 32 29 47 31 48  33 29 45 31 49 38 49 24 29 39 46 34 49 31 33 36 29 38 47 41 45 28  46 34 39 29 40 30 41 52 38 33 39 49 52 . 27 45 29 39 41 30 41 28 31 24  31 37 29 45 31 33 29 45 28 31 42 49 27 45 29 49 40 39 29 30 38 33 39  41 28 28 31 42 31 27 45 29 37 31 35 49 42 .</p>
7)	<p>32 28 39 32 28 47 46 23 28 38 28 36 46 38 29 23 32 30 36 25 21 31 50  46 47 21 35 40 38 46 34 46 36 46 50 43 35 33 36 29 28 51 35 31 29 23  32 46 21 23 33 35 40 29 23 48 28 28 48 23 46 39 21 50 38 21 36 46 48  29 43 46 51 47 46 32 46 50 46 29 38 46 48 38 45 49 32 28 47 46 42 21  49 30 39 35 46 48 , 48 45 43 46 35 38 33 38 28 38 28 35 21 39 44 37  37 33 36 23 21 48 38 46 29 23 21 43 32 21 50 33 38 33 38 21 31 21 32  28 29 29 50 46 23 32 33 38 45 29 43 46 29 46 47 45 51 28 35 40 38 33  24 52 33 34 46 32 28 39 48 21 23 21 31 . 43 32 46 21 39 48 33 51 33 38  28 46 25 33 38 36 28 21 51 33 23 28 35 40 38 45 24 28 38 28 35 21  39 29 30 41 33 29 23 48 30 22 41 21 49 50 46 47 21 35 40 38 45 49 29  38 33 34 46 43 35 28 48 21 35 40 38 45 49 50 28 52 21 38 , 43 32 46 28  38 28 35 21 39 21 32 46 48 28 38 28 43 32 46 47 35 33 50 28 36 28 42  33 29 23 48 28 28 48 23 46 39 21 50 38 21 36 46 48 , 32 28 29 29 50 46  23 32 33 38 45 29 43 46 29 46 47 45 43 46 48 45 52 33 38 21 31 36 28  42 33 29 23 48 28 48 32 33 50 33 38 38 45 49 39 21 50 38 21 49 28 48  23 46 51 46 32 46 34 21 48 45 31 48 35 33 38 38 28 21 47 46 35 33 33  44 37 37 33 36 23 21 48 38 45 24 , 46 43 21 29 28 38 43 32 21 38 25 21  43 32 28 47 46 23 45 43 32 33 51 35 28 34 28 33 50 46 24 36 46 38 29  23 32 30 36 25 21 21 , 51 46 29 23 46 21 38 29 23 48 28 , 43 32 46 48</p>

	<p>33 51 33 38 45 32 28 29 42 33 23 45 46 29 38 46 48 38 45 49 43 28 32  28 50 33 23 32 46 48 23 33 49 38 21 36 21, 43 32 46 21 39 48 33 51 33  38 32 28 29 42 33 23 21 48 45 43 46 35 38 33 38 43 46 51 47 46 32  32 28 47 46 42 21 49 30 39 35 46 48, 28 23 28 36 27 33 32 28 29 29  42 21 23 28 38 50 46 41 38 46 29 23 38 46 24 47 28 35 28 38 29 50 46  47 21 35 40 38 46 34 46 36 46 50 43 35 33 36 29 28.</p>
8)	<p>22 31 35 46 35 25 32 42 23 32 40 31 35 46 22 21 32 34 38 34 46 28 24  34 37 - 35 32 51 34 37 21 37 29 49 24 32 31 50 49 32 46 31 42 32 50 35  38 31 37 22 32 23 43 32 34 31 35 22 37 22 46 34 49 48 42 32 23 32 22  37 39 37 50 39 32 23 34 37 22 38 51 29 23 28 39 37 22 22 47 30 34  37 36 23 32 29 49 37 34 32 31 28 24 46 31 35 49 32 36 30 32 21 32  39 34 37 40 37 23 37 30 34 37 29 37 35 23 46 34 31 42 37 23 35 46. 34  46 37 31 34 37 22 46 34 49 49 46 34 46 21 49 39 46 37 44 45 32 36 34  38 51 42 37 50 46 39 46 35 32 21 32 52 42 32 23 32 22 37 39 37 50, 31  28 41 32 31 35 22 28 47 41 49 51 35 32 51 34 37 21 37 29 49 52 40 37  31 35 46 22 50 49, 34 46 28 24 34 38 51 42 37 21 37 30 32 34 49 52 22  49 31 31 21 32 40 28 32 36 37 52 37 44 21 46 31 35 49 22 38 40 32 21  32 34 38 34 46 42 23 46 22 21 32 34 49 48 23 46 39 22 49 35 49 48 21  37 29 49 31 35 49 50 49 42 32 23 32 22 37 39 37 50 39 32 23 34 37 22  38 51 29 23 28 39 37 22. 23 46 31 31 36 37 35 23 32 34 38 42 32 23  31 42 32 50 35 49 22 38 28 22 32 21 49 24 32 34 49 48 42 37 31 35 46  22 37 50 39 32 23 34 37 22 38 51 29 23 28 39 37 22 22 34 46 42 23  46 22 21 32 34 49 49 42 37 23 35 37 22 46 39 37 22 37 - 24 32 23 34 37  36 37 23 31 50 37 29 37 44 46 31 31 32 52 34 46. 23 46 39 23 46 44 37  35 46 34 38 34 37 22 38 32 49 34 27 37 23 36 46 26 49 37 34 34 38 32  49 34 31 35 23 28 36 32 34 35 38 42 37 40 40 32 23 30 50 49 42 23 49  34 48 35 49 48 23 32 43 32 34 49 48 42 23 49 37 42 35 49 36 49 39 46  26 49 49 29 23 28 39 37 42 37 35 37 50 37 22 49 23 46 39 23 46 44 37  35 50 49 42 21 46 34 37 22 40 37 31 35 46 22 50 49 39 32 23 34 37 22</p>

	38 51 29 23 28 39 37 22 22 28 31 21 37 22 49 48 51 36 28 21 25 35 49 46 29 32 34 35 34 37 31 35 49 .
9)	47 41 51 35 51 23 39 34 35 41 41 37 43 51 34 39 31 43 30 41 51 34 43 44 41 51 47 43 26 37 26 51 35 32 26 26 43 49 24 39 40 51 35 30 45 34 35 47 22 39 31 26 21 52 22 21 35 47 51 43 37 35 51 26 38 26 34 43 47 35 31 31 46 28 41 26 41 51 39 37 40 43 31 51 34 43 22 21 51 39 37 45 39 34 35 51 30 34 46 , 45 34 26 47 39 52 39 31 35 37 35 51 39 37 35 51 26 33 39 41 40 35 21 37 43 52 39 22 23 45 34 43 32 39 41 41 43 47 31 35 42 34 39 47 35 26 43 28 22 35 27 52 39 31 26 21 26 38 43 22 26 34 43 47 35 31 31 43 42 43 45 43 37 39 48 39 31 26 21 , 45 34 43 47 39 52 39 31 43 37 43 52 39 22 26 34 43 47 35 31 26 39 51 39 37 45 39 34 35 51 30 34 31 46 28 47 43 38 52 39 44 41 51 47 26 44 31 35 43 49 24 39 40 51 30 45 34 35 47 22 39 31 26 21 , 51 35 40 27 39 45 34 26 47 39 52 39 31 37 39 51 43 52 34 39 35 22 26 38 35 32 26 26 26 37 26 51 35 32 26 26 43 49 24 39 40 51 35 30 45 34 35 47 22 39 31 26 21 31 35 37 26 40 34 43 40 43 31 51 34 43 22 22 39 34 39 . 30 41 51 34 43 44 41 51 47 43 45 43 38 47 43 22 26 51 45 34 43 47 43 52 26 51 23 43 51 22 35 52 40 30 26 45 34 43 47 39 34 40 30 35 47 51 43 37 35 51 26 38 26 34 43 47 35 31 31 46 28 41 26 41 51 39 37 40 43 31 51 34 43 22 21 51 39 37 45 39 34 35 51 30 34 46 47 22 35 49 43 34 35 51 43 34 31 46 28 30 41 22 43 47 26 21 28 , 33 51 43 45 43 47 46 41 26 51 40 35 33 39 41 51 47 43 34 35 38 34 35 49 35 51 46 47 35 39 37 46 28 41 26 41 51 39 37 40 43 31 51 34 43 22 21 51 39 37 45 39 34 35 51 30 34 46 .
10)	38 36 43 41 51 37 49 47 29 29 38 24 29 25 49 38 43 36 39 31 28 30 41 35 37 25 49 42 23 35 29 22 37 49 38 28 31 28 41 33 36 37 38 23 29 41 31 37 38 37 37 52 24 43 42 37 38 43 51 29 31 33 36 23 29 25 37 32 29 31 28 , 35 37 51 37 24 23 29 38 23 42 23 38 43 26 51 28 36 51 29 24 29 41 44 41 22 29 50 28 43 31 28 41 51 37 38 . 50 29 31 33 32 43 36 36 37 30 41 51 43 51 33 28 – 24 43 41 41 25 37 51 24 29 51 33 37 41

	<p>36 37 38 36 23 29 41 22 37 41 37 52 23 41 31 37 38 37 37 52 24 43 42  37 38 43 36 28 49 38 41 37 38 24 29 25 29 36 36 37 25 43 36 39 31 28  30 41 35 37 25 49 42 23 35 29 28 22 24 37 43 36 43 31 28 42 28 24 37  38 43 51 33 41 31 37 38 37 37 52 24 43 42 37 38 43 51 29 31 33 36 23 29  25 37 32 29 31 28 . 43 38 51 37 24 23 24 43 52 37 51 23 38 24 43 25  35 43 48 32 43 36 36 37 30 41 51 43 51 33 28 28 41 22 37 31 33 42 44  26 51 51 43 35 37 30 25 29 51 37 32 , 35 43 35 35 37 39 36 28 51 28  38 36 37 - 41 29 25 43 36 51 28 27 29 41 35 28 30 . 51 43 35 21 29 43  36 43 31 28 42 41 31 37 38 37 37 52 24 43 42 37 38 43 36 28 49 38 41  37 38 24 29 25 29 36 36 37 25 43 36 39 31 28 30 41 35 37 25 49 42 23  35 29 28 32 29 51 36 43 37 41 36 37 38 29 28 42 44 27 29 36 28 49  52 43 42 23 37 51 29 27 29 41 51 38 29 36 36 23 48 28 42 43 24 44 52  29 21 36 23 48 36 43 44 27 36 23 48 51 24 44 32 37 38 , 35 37 51 37  24 23 29 36 43 22 24 43 38 31 29 36 23 36 43 28 41 41 31 29 32 37 38  43 36 28 29 36 29 37 31 37 39 28 42 25 37 38 38 43 36 39 31 28 30 41  35 37 25 49 42 23 35 29 . 22 37 25 28 25 37 45 51 37 39 37 , 38 41  51 43 51 33 29 22 24 28 38 29 32 29 36 23 32 43 36 36 23 29 37 22 24  37 41 43 28 36 40 37 24 25 43 36 51 37 38 28 36 43 52 31 26 32 29 36  28 49 43 38 51 37 24 37 38 , 35 37 51 37 24 23 29 52 23 31 28 22 37  31 44 27 29 36 23 22 24 28 22 37 41 29 47 29 36 28 28 38 29 31 28 35  37 52 24 28 51 43 36 28 28 38 2010 - 2020 39 39 .</p>
11)	<p>41 23 51 35 51 39 45 33 35 23 23 38 50 51 33 45 49 47 50 23 49 50 41  49 47 45 42 50 28 27 50 28 47 25 50 33 46 35 49 34 21 35 24 34 34 26  25 50 52 50 46 34 31 45 23 25 50 46 50 44 42 33 35 41 52 45 49 34 32  34 50 40 45 23 42 45 31 45 49 34 32 26 25 50 52 50 46 34 31 45 23 25  50 48 40 45 21 50 42 35 23 49 50 23 51 34 49 35 42 33 34 38 47 36 52  45 49 49 47 27 42 33 45 28 42 33 34 32 51 34 32 27 33 50 23 23 34 34 ,  41 47 28 45 52 45 49 47 25 52 30 31 45 41 47 45 42 33 50 40 52 45 38  47 34 51 45 49 28 45 49 24 34 34 26 25 50 52 50 46 34 31 45 23 25 50</p>

	<p>46 50 38 45 49 45 28 22 38 45 49 51 35 41 42 33 50 38 47 36 52 45 49  49 50 23 51 34 , 37 35 25 51 50 33 47 34 44 23 52 50 41 34 32 50 40  45 23 42 45 31 45 49 34 32 26 25 50 52 50 46 34 31 45 23 25 50 48 40  45 21 50 42 35 23 49 50 23 51 34 42 33 50 34 21 41 50 28 23 51 41 45 49  49 50 48 23 37 45 33 47 . 49 35 50 23 49 50 41 45 25 50 38 42 52 45  25 23 49 50 46 50 35 49 35 52 34 21 35 49 35 44 31 49 50 48 52 34 51  45 33 35 51 44 33 47 34 28 45 32 51 45 52 39 49 50 23 51 34 42 50 50  40 45 23 42 45 31 45 49 34 30 33 45 35 52 34 21 35 24 34 34 26 25 50  52 50 46 34 31 45 23 25 50 46 50 44 42 33 35 41 52 45 49 34 32 25 33  44 42 49 47 27 42 33 50 38 47 36 52 45 49 49 47 27 42 33 45 28 42 33  34 32 51 34 48 23 51 33 35 49 47 , 41 47 32 41 52 45 49 47 50 23 49  50 41 49 47 45 49 35 42 33 35 41 52 45 49 34 32 34 42 33 50 40 52 45  38 47 42 33 35 25 51 34 31 45 23 25 50 48 33 45 35 52 34 21 35 24 34  34 26 25 50 52 50 46 34 31 45 23 25 50 46 50 38 45 49 45 28 22 38 45  49 51 35 , 35 51 35 25 22 45 42 33 50 45 25 51 34 33 50 41 35 49 34  32 34 37 44 49 25 24 34 50 49 34 33 50 41 35 49 34 32 23 34 23 51 45  38 26 25 50 52 50 46 34 31 45 23 25 50 48 40 45 21 50 42 35 23 49 50  23 51 34 41 42 33 50 38 47 36 52 45 49 49 50 48 23 37 45 33 45 .</p>
12)	<p>40 52 21 38 43 35 29 32 45 45 40 28 45 31 29 47 45 38 34 25 46 35 43  52 25 48 25 38 34 35 46 22 39 44 45 43 38 29 40 35 31 52 35 49 25 41  38 25 43 44 21 37 25 29 41 , 48 35 49 42 21 34 25 46 35 43 25 28 44 45  31 50 23 34 35 46 45 43 38 36 25 43 21 45 43 38 29 38 46 35 30 52 50  31 , 38 46 25 26 48 35 31 28 25 38 48 35 40 21 52 52 50 31 25 46 25  40 52 45 48 35 43 35 28 50 41 38 46 44 36 21 29 41 52 45 40 35 39 31  35 30 52 50 31 . 40 34 35 38 46 45 42 52 25 45 49 35 42 50 , 47 45 38  34 25 46 35 43 52 25 48 25 ( 42 28 35 52 50 ) 38 43 21 46 25 35 36 45  52 22 34 35 34 44 46 29 28 52 50 31 25 , 47 46 21 49 35 42 21 28 29 34  28 35 38 43 35 43 45 25 38 34 35 46 22 39 35 40 21 52 25 29 25 38 40  35 45 23 44 52 25 40 45 28 38 21 46 22 52 35 38 43 25 . 21 48 43 44 21</p>

	<p>46 22 52 35 38 43 22 39 21 42 21 36 25 38 25 52 43 45 39 21 38 25 38  43 45 31 44 34 28 21 40 46 45 52 25 29 47 45 38 34 25 46 35 43 52 50  31 46 45 43 21 43 45 46 22 52 50 31 21 34 34 21 28 21 43 35 31 41 21  28 21 48 43 45 28 25 39 44 45 43 38 29 38 46 35 30 52 35 38 43 22 24  25 41 31 21 43 45 31 21 43 25 36 45 38 48 35 23 31 35 42 45 46 25 25  47 35 46 22 26 25 31 36 25 38 46 35 31 27 48 38 34 45 28 25 31 45 52  43 21 46 22 52 35 35 34 28 45 42 45 46 29 45 31 50 41 34 21 28 21 31  45 43 28 35 40 . 40 42 21 52 52 35 23 38 43 21 43 22 25 34 28 45 42  46 35 30 45 52 21 31 45 43 35 42 25 48 21 34 28 35 45 48 43 25 28 35  40 21 52 25 29 31 35 42 45 46 25 38 25 38 43 45 31 50 28 45 49 44 46  25 28 35 40 21 52 25 29 38 52 45 36 45 43 48 25 31 46 35 49 25 36 45  38 48 25 31 48 35 52 43 28 35 46 46 45 28 35 31 . 34 28 25 40 45 42 45  52 50 28 45 39 44 46 22 43 21 43 50 25 31 25 43 21 37 25 35 52 52 35  49 35 31 35 42 45 46 25 28 35 40 21 52 25 29 38 25 38 43 45 31 50 38  52 45 36 45 43 48 25 31 46 35 49 25 36 45 38 48 25 31 48 35 52 43 28  35 46 46 45 28 35 31 .</p>
13)	<p>34 28 47 21 47 51 25 26 21 28 28 35 21 47 26 42 34 21 43 47 28 23 27  21 30 21 39 42 , 34 33 27 40 42 45 21 43 46 42 25 49 26 42 26 21 28  49 33 27 40 21 34 21 40 42 42 33 36 26 21 27 33 34 , 28 34 23 27 21 40  40 37 25 28 45 44 21 28 47 25 26 42 27 21 32 42 25 31 42 21 36 28  47 26 21 45 32 42 25 31 30 21 40 40 37 50 . 30 25 47 21 44 42 27 42 26  33 34 21 40 37 47 42 49 33 34 37 25 34 21 26 42 21 40 47 37 45 44 21  28 47 25 26 42 27 21 32 42 42 30 21 40 40 37 50 . 49 26 42 34 25 30 25  40 21 27 21 30 21 39 21 49 26 25 33 36 26 21 27 33 34 21 40 42 23 30  21 40 40 37 50 35 25 47 33 30 33 35 34 25 45 47 33 26 40 33 48 33 45  34 21 40 47 33 34 21 40 42 23 28 40 21 42 35 25 40 51 22 25 31 33 22  42 36 45 33 31 . 33 49 42 28 21 40 21 28 42 28 47 25 35 21 45 33 40  45 24 26 25 40 47 40 33 48 33 33 36 24 39 25 40 42 23 42 28 45 24 28  28 47 34 25 40 40 33 31 40 25 31 26 33 40 40 33 31 28 25 47 42 40 21</p>

	<p>33 28 40 33 34 25 26 21 28 47 24 46 25 48 33 40 25 31 26 33 40 40 33  48 33 48 21 27 21 . 42 28 49 33 44 51 27 24 23 35 25 47 33 30 26 21  28 47 24 46 25 48 33 40 25 31 26 33 40 40 33 48 33 48 21 27 21 49 26  25 30 44 33 41 25 40 24 44 24 39 22 25 40 40 37 31 21 44 48 33 26 42  47 35 28 21 35 33 33 36 24 39 21 43 46 25 31 28 23 42 28 45 24 28 28  47 34 25 40 40 33 31 40 25 31 26 33 40 40 33 31 28 25 47 42 45 33 40  45 24 26 25 40 47 40 33 48 33 33 36 24 39 25 40 42 23 . 33 49 26 25 30  25 44 25 40 37 45 26 42 47 25 26 42 42 27 21 34 25 26 22 25 40 42 23  45 44 21 28 47 25 26 42 27 21 32 42 42 28 42 28 49 33 44 51 27 33 34  21 40 42 25 35 45 26 42 47 25 26 42 23 21 30 21 49 47 21 32 42 42 34  45 21 39 25 28 47 34 25 45 26 42 47 25 26 42 23 33 28 47 21 40 33 34  45 42 . 49 26 42 34 25 30 25 40 37 49 26 42 35 25 26 37 45 44 21 28  47 25 26 42 27 21 32 42 42 30 21 40 40 37 50 42 28 45 24 28 28 47 34  25 40 40 33 31 40 25 31 26 33 40 40 33 31 28 25 47 51 43 35 25 47 33  30 33 35 26 21 28 47 24 46 25 48 33 40 25 31 26 33 40 40 33 48 33 48  21 27 21 .</p>
14)	<p>52 43 22 43 38 24 31 32 52 39 24 41 42 30 22 37 52 52 49 42 25 32 39  22 30 37 46 31 45 32 47 49 42 33 28 30 22 45 23 26 42 30 37 24 39 40  22 37 33 32 25 42 29 52 43 39 37 24 43 32 36 32 31 45 37 42 33 30 37 36  32 39 48 49 42 36 43 45 32 39 32 40 32 39 48 49 42 36 43 45 37 35 37  21 37 45 32 39 22 30 30 28 27 50 42 49 42 40 30 28 27 25 32 45 32 44  52 36 32 30 43 22 36 43 30 28 33 31 45 32 39 32 25 32 33 , 52 32 31  45 32 39 32 50 25 22 46 41 42 44 32 52 24 39 32 40 30 37 36 30 32 39 42  30 37 42 33 48 49 42 36 43 45 37 51 42 52 36 32 29 25 23 44 37 . 52  21 42 49 38 46 25 22 49 38 30 42 29 26 42 44 32 45 22 40 39 37 43 37  24 52 37 52 43 42 33 28 43 42 27 30 37 51 42 52 36 32 29 25 37 22 44  30 32 52 43 37 36 37 30 22 45 23 26 42 30 37 29 43 32 36 32 52 34 42  33 22 , 52 32 31 45 32 39 32 50 25 22 42 33 28 27 25 23 44 32 32 47 45  22 40 32 39 22 30 37 42 33 , 30 42 32 47 27 32 25 37 33 32 37 52 52 49</p>

	<p>42 25 32 39 22 30 37 42 27 22 45 22 36 43 42 45 22 37 31 22 45 22 33  42 43 45 32 39 31 45 32 21 42 52 52 32 39 , 31 45 32 37 52 27 32 25 24  41 37 27 31 45 37 25 22 30 30 28 27 30 22 45 23 26 42 30 37 24 27 .  32 52 30 32 39 30 22 24 51 22 52 43 38 52 43 22 43 38 37 31 32 52 39  24 41 42 30 22 39 32 31 45 32 52 23 32 31 45 42 25 42 49 42 30 37 24  44 42 32 33 42 43 45 37 51 42 52 36 37 27 31 22 45 22 33 42 43 45 32 39  32 47 49 22 52 43 37 30 22 44 45 42 39 22 33 22 43 42 45 37 22 49 22  36 32 30 43 22 36 43 30 32 44 32 31 45 32 39 32 25 22 25 39 37 50 23  41 42 29 52 24 48 49 42 36 43 45 37 51 42 52 36 32 29 25 23 44 32 29  52 31 32 52 49 42 25 23 46 41 37 33 22 30 22 49 37 40 32 33 31 45 37  33 42 30 37 33 32 52 43 37 31 32 49 23 51 42 30 30 28 27 40 22 39 37  52 37 33 32 52 43 42 29 37 37 27 30 32 45 33 37 45 32 39 22 30 37 42  33 .</p>
15)	<p>36 28 44 36 28 47 27 46 28 48 21 31 28 46 26 31 28 46 50 45 26 22 30 28  38 31 27 49 26 32 37 50 28 32 52 27 36 50 46 31 39 36 27 52 36 28  31 31 48 27 23 36 26 28 32 50 44 28 43 50 50 48 28 44 48 28 45 26 48  50 38 39 36 50 27 36 50 46 26 46 27 24 24 21 39 27 32 48 38 26 31 21  31 24 50 48 29 27 36 31 28 43 50 27 48 48 27 23 22 50 22 46 26 31 26  50 25 28 36 28 30 46 26 36 50 44 34 26 31 21 31 36 38 49 27 31 22 24  27 23 22 46 24 44 28 49 28 45 28 31 . 28 32 52 27 36 50 46 31 39 36  26 49 22 46 28 24 32 26 48 22 32 27 24 26 22 48 27 50 24 24 50 49  26 47 32 27 30 - 22 25 26 31 21 . 39 36 50 36 28 44 36 28 47 27 46 30  26 31 27 49 26 32 50 50 22 39 27 32 37 44 27 24 28 32 50 22 37 46 26  27 36 50 38 39 36 50 48 38 46 50 38 36 26 35 26 48 50 23 , 28 32 52  26 47 36 28 32 27 52 50 30 50 , 46 26 27 36 50 38 27 46 48 27 35 26  48 50 23 50 46 26 27 36 50 38 31 48 27 40 26 22 46 24 . 36 28 48 40  50 36 27 24 28 48 50 26 39 27 22 46 36 34 30 46 34 36 48 27 31 34 30  36 50 46 26 36 50 33 39 27 44 24 27 32 38 26 46 27 47 51 26 49 50 48  38 46 37 44 28 49 28 45 50 , 27 46 48 27 22 38 41 50 26 22 38 30 36</p>



	<p>28 44 48 21 31 39 36 50 32 27 40 26 48 50 38 31 , 24 52 36 34 39 39  21 22 27 49 50 48 28 30 27 24 21 31 39 36 50 27 36 50 46 26 46 27 31  , 45 46 27 39 27 24 21 35 28 26 46 42 29 29 26 30 46 50 24 48 27 22  46 37 50 48 29 27 36 31 28 43 50 27 48 48 27 - 24 21 45 50 22 32 50 46  26 32 37 48 27 23 22 50 22 46 26 31 21 . 36 26 44 34 32 37 46 28 46 21  39 27 49 46 24 26 36 40 49 26 48 21 24 25 27 49 26 50 31 50 46 28 43  50 27 48 48 27 52 27 31 27 49 26 32 50 36 27 24 28 48 50 38 50 46 26  22 46 50 36 27 24 28 48 50 38 .</p>
16)	<p>39 43 35 33 24 25 27 51 29 29 38 27 23 24 39 35 26 31 49 43 24 21 27  29 29 31 52 51 23 28 24 40 35 50 26 24 48 44 49 51 25 35 28 29 51 51  26 24 39 24 46 24 37 35 25 27 43 51 35 38 35 51 26 40 43 35 28 43 35  29 26 24 48 24 49 25 24 44 38 27 28 25 43 24 26 51 28 51 - 35 43 29  27 26 51 23 35 51 26 23 51 34 , 38 27 46 51 43 24 39 35 26 26 24 46 24  39 51 29 37 45 25 24 37 49 43 51 51 29 49 24 38 42 50 24 39 35 26 51  51 29 25 45 49 27 26 30 35 25 24 46 24 25 27 49 38 24 39 24 46 24 49  24 38 34 . 49 43 24 39 27 23 27 26 35 26 35 38 51 50 43 35 39 26 24  39 27 29 51 34 40 35 50 39 49 43 24 21 27 29 29 27 43 24 29 25 35  25 39 27 43 23 24 46 24 43 35 29 25 39 24 43 35 . 49 24 28 35 50 35 26  35 39 24 50 37 24 52 26 24 29 25 42 40 24 43 37 51 43 24 39 35 26 51  34 37 27 50 24 29 25 43 45 28 25 45 43 31 ( 37 24 23 45 38 34 21 51 51  29 24 29 25 35 39 35 49 24 28 24 24 43 23 51 26 35 25 27 43 24 29 25  35 ) . 43 35 29 29 37 24 25 43 27 26 31 49 43 24 33 38 27 37 31 23 27  40 27 28 25 24 24 33 43 35 50 24 39 35 26 51 34 39 28 24 37 49 24 50  51 25 26 31 36 29 38 24 34 36 , 39 31 43 35 22 27 26 26 31 36 51 50  43 35 29 49 38 35 39 35 . 24 33 29 45 52 23 35 41 25 29 34 49 45 25 51  45 37 27 26 42 47 27 26 51 34 49 38 24 25 26 24 29 25 51 23 51 29 38  24 28 35 21 51 48 39 46 43 35 23 51 27 26 25 26 31 36 29 38 24 34 36  . 43 35 50 43 35 33 24 25 35 26 24 25 26 24 29 51 25 27 38 42 26 24 26  27 29 38 24 52 26 31 48 29 49 24 29 24 33 45 49 43 35 39 38 27 26 51</p>

	<p>34 25 27 49 38 24 39 31 37 49 24 38 27 37 25 27 37 49 27 43 35 25 45  43 31 39 50 24 26 27 28 43 51 29 25 35 38 38 51 50 35 21 51 51 51  26 24 39 35 34 25 27 36 26 24 38 24 46 51 30 27 29 28 35 34 49 43 24  21 27 23 45 43 35 49 24 29 38 27 23 24 39 35 25 27 38 42 26 24 48 28  43 51 29 25 35 38 38 51 50 35 21 51 51 25 39 27 43 23 31 36 43 35 29  25 39 24 43 24 39 29 37 27 50 24 29 25 43 45 28 25 45 43 24 48 .</p>
17)	<p>36 43 37 41 49 21 48 21 37 47 32 33 40 34 28 21 33 27 49 21 32 32 23  24 23 27 21 26 23 33 22 37 47 34 41 34 28 36 34 32 47 43 34 37 40 23  33 48 43 21 24 34 28 28 34 43 34 40 34 48 34 40 21 27 21 43 47 21  42 , 36 43 37 41 32 47 21 28 49 37 40 40 25 42 47 34 44 37 44 40 25 22  23 23 36 34 49 23 48 34 40 21 49 46 40 25 22 23 36 43 37 36 33 47 32  47 28 23 33 22 23 . 23 32 42 34 41 33 23 29 47 34 36 34 49 34 48 23  23 36 43 34 32 47 43 21 40 32 47 28 21 36 43 37 41 49 21 48 21 37 47  32 33 27 49 21 32 32 23 24 23 26 23 43 34 28 21 47 46 36 34 32 47 43  34 37 40 40 25 37 48 43 21 24 25 28 34 43 34 40 34 48 34 27 21 27 28  40 37 50 40 23 37 23 28 40 45 47 43 37 40 40 23 37 . 47 21 27 23 22  34 39 43 21 29 34 22 , 22 37 47 34 41 25 36 34 32 47 43 34 37 40 23 33  48 43 21 24 34 28 28 34 43 34 40 34 48 34 22 34 48 45 47 43 21 32 32  44 23 47 25 28 21 47 46 49 23 39 34 34 41 23 40 23 29 36 43 37 41  32 47 21 28 49 37 40 40 25 42 47 23 36 34 28 48 43 21 24 34 28 28 34  43 34 40 34 48 34 , 49 23 39 34 34 39 21 47 23 36 21 . 28 28 37 41 37  40 40 25 37 36 34 40 33 47 23 33 23 36 43 37 41 49 21 48 21 37 22 21  33 27 49 21 32 32 23 24 23 27 21 26 23 33 39 45 41 45 47 36 34 49 37  29 40 25 41 49 33 23 32 32 49 37 41 34 28 21 47 37 49 37 52 - 43 34 39  34 47 34 47 37 42 40 23 27 34 28 , 23 32 36 34 49 46 29 45 51 38 23 42  22 37 47 34 41 48 43 21 24 21 28 34 43 34 40 34 48 34 36 43 23 36  49 21 40 23 43 34 28 21 40 23 23 36 45 47 23 22 34 39 23 49 46 40 25  42 43 34 39 34 47 34 28 28 43 21 29 49 23 44 40 25 42 32 43 37 41  21 42 .</p>

18)	<p>47 40 39 38 42 44 42 47 34 34 48 47 39 42 23 40 47 24 39 40 28 23 51  43 23 26 37 47 49 39 38 42 47 34 26 32 38 43 43 38 34 39 23 43 47 47  42 46 23 39 26 49 39 25 42 43 44 26 23 27 28 47 43 23 42 38 40 38 41  43 44 26 42 26 45 26 43 23 51 22 38 34 39 23 43 23 41 43 44 46 32 21  47 43 23 35 41 26 42 43 38 48 38 42 34 49 38 22 38 27 38 52 26 42 26  30 29 51 49 42 47 34 43 38 21 47 42 34 49 38 22 38 49 42 47 51 . 40  44 51 40 28 26 43 44 49 28 23 48 47 39 23 41 26 34 49 23 26 23 34 38  33 23 47 28 29 43 38 - 31 49 38 43 38 48 23 41 26 34 49 23 26 25 34 28  38 40 23 51 21 47 43 43 38 22 38 42 26 22 23 38 43 47 . 38 27 42 26  21 26 28 26 43 44 42 26 30 23 48 44 31 49 34 27 28 25 47 39 47 33 23  23 32 21 47 43 23 35 , 21 23 49 39 25 26 48 44 26 49 28 23 48 47 39  23 41 26 34 49 23 48 23 46 47 42 47 49 39 26 42 23 34 39 23 49 47 48 23  . 38 27 39 23 48 47 28 29 43 44 48 42 26 45 26 43 23 26 48 21 28 51  21 47 43 43 38 22 38 42 26 22 23 38 43 47 51 40 28 51 26 39 34 51 32  21 47 43 23 26 49 42 25 22 28 38 22 38 21 23 41 43 38 22 38 23 34 27  38 28 29 32 38 40 47 43 23 51 , 23 48 26 24 50 26 26 34 26 32 38 43 43  38 26 42 47 34 45 23 42 26 43 23 26 . 47 40 39 38 42 44 38 27 23 34  44 40 47 24 39 42 26 45 26 43 23 51 43 38 48 26 42 38 40 23 38 52  50 26 34 39 40 26 43 43 44 46 27 42 38 34 39 42 47 43 34 39 40 22 38  34 39 23 43 23 33 , 25 41 23 39 44 40 47 24 50 23 26 34 26 32 38 43 43  44 26 23 32 48 26 43 26 43 23 51 40 48 26 34 39 23 48 38 34 39 23 , 43  47 32 43 47 41 26 43 23 51 27 38 48 26 50 26 43 23 51 , 27 42 23 42 38  21 43 38 - 49 28 23 48 47 39 23 41 26 34 49 23 26 23 21 42 25 22 23 26  37 47 49 39 38 42 44 .</p>
19)	<p>28 42 42 21 47 22 51 47 41 42 24 35 26 41 47 35 26 41 28 52 47 42 50 26  24 35 45 22 47 21 43 42 45 34 21 26 42 45 37 26 29 28 24 52 26 42 41  29 27 31 28 45 44 46 47 42 41 37 47 29 29 27 31 28 29 41 47 48 47 42  45 37 25 48 28 37 29 47 22 48 47 29 28 28 28 29 29 45 37 26 32 28 40  37 42 21 51 52 26 47 29 47 42 50 45 21 43 50 28 31 26 34 47 29 41 45</p>

	<p>37 . 51 52 28 41 27 37 26 47 41 42 24 29 26 21 28 52 28 47 22 37 51  31 51 48 45 37 29 47 40 51 25 48 26 37 21 47 29 28 24 , 37 48 45 21  28 50 45 41 45 48 27 31 37 27 42 41 51 25 26 30 41 42 51 25 47 48 37  26 40 49 47 48 28 29 47 42 50 45 21 43 50 45 26 34 47 29 41 45 37 .  45 41 29 45 38 47 29 28 24 35 47 36 22 51 42 51 25 47 48 37 26 40 49  47 48 45 35 28 26 34 47 29 41 26 35 28 42 41 48 45 24 41 42 24 29  26 45 42 29 45 37 47 28 47 48 26 48 31 28 28 37 42 45 45 41 37 47  41 42 41 37 28 28 42 28 29 33 45 48 35 26 32 28 45 29 29 27 35 28 48  47 34 21 26 35 47 29 41 26 35 28 28 34 48 38 41 26 50 47 21 43 44 47  48 34 26 . 37 50 26 52 47 42 41 37 47 35 47 41 45 22 26 28 47 48 26  48 31 28 52 47 42 50 45 34 45 51 25 48 26 37 21 47 29 28 24 28 42 25  45 21 43 49 51 47 41 42 24 35 47 41 45 22 25 45 44 51 36 22 47 29 28  24 . 51 50 26 49 26 29 27 26 21 34 45 48 28 41 35 27 25 45 42 41 48  45 47 29 28 24 48 26 37 29 45 37 47 42 28 40 22 21 24 48 26 49 29 27  31 28 29 33 45 48 35 26 32 28 45 29 29 27 31 48 47 34 21 26 35 47 29  41 45 37 . 52 28 42 21 47 29 29 26 24 48 47 26 21 28 49 26 32 28 24 25  48 47 22 21 45 36 47 29 29 27 31 26 21 34 45 48 28 41 35 45 37 45 42  29 45 37 26 29 26 29 26 28 35 28 41 26 32 28 45 29 29 45 35 35 45 22  47 21 28 48 45 37 26 29 28 28 . 22 26 29 26 29 26 21 28 49 25 45 21  51 52 47 29 29 27 31 48 47 49 51 21 43 41 26 41 45 37 .</p>
20)	<p>27 23 26 46 38 29 26 35 46 47 23 38 42 47 28 38 38 21 41 35 26 28 29  33 33 29 33 21 26 29 36 30 29 37 40 29 48 45 23 26 33 40 38 26 34 35  47 24 47 32 40 33 37 50 43 33 48 43 46 47 27 , 33 21 37 42 47 23 23  25 27 33 30 26 33 40 47 21 50 26 36 35 47 42 48 38 51 23 25 31 50  47 40 29 46 26 35 38 36 46 35 43 42 26 21 . 42 47 41 35 26 28 29 33  33 41 29 35 29 27 29 24 29 23 38 37 23 29 26 34 31 26 30 38 27 26 46  26 50 26 48 38 51 29 33 40 21 47 46 35 43 42 47 21 42 47 30 47 23  23 43 32 40 26 51 50 43 33 38 33 41 26 48 45 42 26 21 47 23 38 29 27  26 41 40 38 27 47 48 45 23 26 46 26 27 47 35 22 35 43 40 47 26 40 21</p>

29 51 47 29 40 40 35 47 23 33 41 26 35 40 23 47 37 48 26 46 38 33 40  
38 50 47 . 41 35 38 52 40 26 27 , 51 47 33 40 26 21 26 42 23 38 50 47  
29 40 30 26 41 26 48 23 38 40 29 48 45 23 26 29 26 46 35 47 23 38 51  
29 23 38 29 - 30 26 33 40 47 21 50 47 46 35 43 42 47 21 42 47 30 47  
23 23 43 32 40 26 51 50 43 30 26 48 49 23 26 26 33 43 24 29 33 40 21  
48 37 40 45 33 37 33 40 35 26 46 26 21 40 29 51 29 23 38 29 26 41  
35 29 30 29 48 29 23 23 26 46 26 21 35 29 27 29 23 23 26 46 26 38 23  
40 29 35 21 47 48 47 , 40 26 29 33 40 45 21 35 29 27 29 23 23 26 29  
26 50 23 26 . 23 47 48 38 51 38 29 21 35 29 27 29 23 23 25 31 26 50  
26 23 41 35 38 21 26 30 38 40 50 40 26 27 43 , 51 40 26 33 44 26 35  
27 38 35 26 21 47 23 23 25 29 34 29 42 38 31 43 51 29 40 47 27 47  
35 22 35 43 40 25 23 29 37 21 48 37 32 40 33 37 30 26 41 43 33 40 38  
27 25 27 38 . 21 35 47 27 50 47 31 30 47 23 23 26 36 33 40 47 40 45  
38 35 47 33 33 27 47 40 35 38 21 47 29 40 33 37 35 47 42 35 47 34 26  
40 50 47 33 26 34 33 40 21 29 23 23 26 46 26 21 47 35 38 47 23 40 47  
35 29 22 29 23 38 37 42 47 30 47 51 38 41 48 47 23 38 35 26 21 47 23  
38 37 38 26 41 40 38 27 38 42 47 28 38 38 27 47 35 22 35 43 40 47 33  
43 51 29 40 26 27 21 35 29 27 29 23 23 25 31 26 50 26 23 .

### **Содержание отчета**

- 1) Титульный лист (Пример в приложении В).
- 2) Цель работы.
- 3) Таблицы, вычисления, примеры расчетов, диаграммы.
- 4) Расшифрованный текст.
- 5) Выводы.

### **Контрольные вопросы**

- 1) Чем шифрование отличается от кодирования?
- 2) Должен ли быть секретным алгоритм шифрования?
- 3) Должен ли быть секретным ключ шифра при симметричном шифровании?
- 4) Кто может знать алгоритм шифрования?

- 5) Кто должен знать ключ шифра?
- 6) Что делать, если размер ключа меньше размера текста?
- 7) В чем заключается идея шифра простой замены?
- 8) Алфавиты открытого текста и шифртекста совпадают или отличаются?
- 9) Как соотносятся частоты появления открытого текста и шифротекста?
- 10) Сколько уникальных вариантов ключа можно получить для заданного размера блока?

### **Литература**

- 1) Титов, А. А. Инженерно-техническая защита информации: учебное пособие / А. А. Титов. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/13931.html>. — Режим доступа: для авторизир. Пользователей
- 2) Литвинов, Р. В. Технические средства защиты информации. Часть 1: курс лекций / Р. В. Литвинов, К. А. Волегов, А. П. Бацула. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2006. — 170 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/14027.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей
- 3) Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 95 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17925.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

4) Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 104 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17926.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

## **Тема 4. Методы защиты информации с применением симметричных алгоритмов шифрования**

### **Лабораторная работа №2 «Изучение математических моделей шифра Виженера и численных методов его реализации»**

**Цель работы:** изучить принципы шифрования и дешифрования информации с применением шифра Виженера, а также математическую модель шифра.

#### **Программа работы**

- 1) Изучить теоретический материал, математические и алгоритмические особенности шифра Виженера.
- 2) В соответствии с заданием расшифровать текст, закодированный шифром Виженера.

#### **Элементы теории**

Шифр Виженера – это метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Суть алгоритма шифрования проста. Шифр Виженера — это набор шифров Цезаря с различными значениями сдвига.

Шифрование этим методом осуществляется в соответствии с таблицей, представляющей собой квадратную матрицу размерностью  $n \times n$ , где  $n$  - число символов используемого алфавита.

В таблице 2.1 показана таблица Виженера для букв русского алфавита (32 буквы и знак пробела). Первая строка матрицы содержит все символы используемого алфавита. Каждая последующая строка получается из предыдущего циклическим сдвигом в влево, но один символ.



Таблица 2.1 – Матрица Виженера для алфавита 32 символа и пробела

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

Для шифрования этим методом необходимо выбрать ключевое слово или ключевую фразу. Алгоритм шифрования, следующий:

- под исходным текстом записываются буквы ключа, если ключевое слово или фраза короче текста, то его применяют несколько раз;

– буквы шифротекста находятся на пересечении столбца таблицы, определяемого в соответствии с открытым текстом строки определяемого буквой ключа.

Пример шифрования:

Требуется зашифровать следующее сообщение: «ПРИВЕТ\_МИР». С помощью ключа «НОТА» записывается открытый текст с циклически повторяемым ключом под ней:

П Р И В Е Т \_ М И Р  
 Н О Т А Н О Т А Н О

Процесс шифрования показан на рисунке 2.1, а в результате шифрования получится сообщение: БЮЪВТ\_СМХЮ.

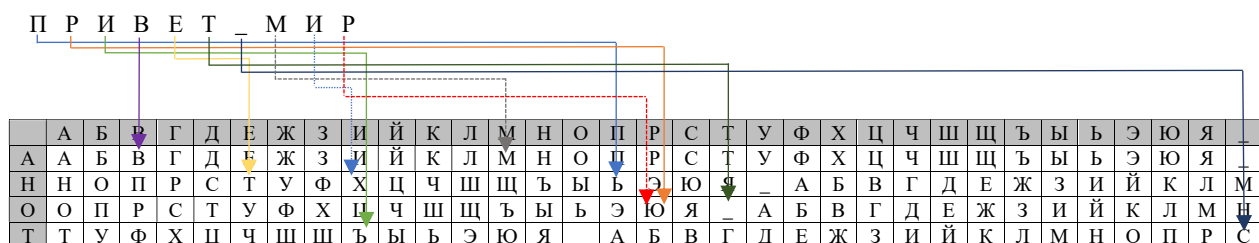


Рисунок 2.1 – Процесс замены букв шифром Виженера

Расшифровывание текста происходит в обратном порядке.

**Пример криптоанализа шифра Виженера**

Дан шифротекст, закодированный шифром Виженера, требуется найти ключевое слово и расшифровать текст.

Шифрованный текст:

ЩЩБЧХУЭЙРУКЧЪЖЭЗПЫБМПКВЪЙЪЕБЕШЦСЛЯХЦОТЙПНДРЛЦ  
 ЯЦКАДХЦОДЦКЛШГЙ\_ЯХЛЭДЧЛЭНЬЦЭБУКРЭТШЮИЕККЪЙ\_ЛНПЭ  
 ОХЙУЭЗЪЛИЧЙЪНДВЛПТЫЙЭЗЙЦПМШЧЭЯЙЧЮИПЫЩФЙЦКЯЙРВ  
 ЦЩЩУЪХЩ\_ЧХУЭЯЙЪЛЦШМШАЧЩ\_БЧУЫЦЦЮЪШЬИДМУИЯЙЩК  
 ЧЙБРИЕККЪЙТЮЕХЛЗЧХЛЭЪУХЪХК\_ЦЫНЛФЙХЛВЧЛПЙЙЩКЧЙХЕ  
 ГЭЦЮЗЕК\_ЦФЫВЗХЛЭЯЙТЮБТЦЮЗЕКОБПТЮВТКЪМЮХАККРЪШН  
 ЮЖТНЮБККВЪЙЮЕШХЛЯЪЖОХЙУЭДЛЦБЖТЭЦЦИК\_ЗПКЯСХЩЭ

ЪШЭЛЩШКФЪРДЦЩЩИНКЪЮЦЦЛХЧЙПЛБРШЮЦЛЕИЧЙШЮЩЫР  
АЫККЛЗЪЛ\_ЯЪЖЭЖШПЕИПЦЦЗФУЖЦОЩЙЦЫНЛФЙХЛВЧЛПЙЙЭЕЛ  
ЭИЭЫПНЕНПЪЗЙЗКГЯСШЩЦЧЛЭЫМЩНЪЙМШБККЙЪЪРИТЙНВИПЫ  
ЭЩДЦЭЗЪЛ\_ГТКПЖИЪИЯЪЖЭЯЙЪПЙАЛИЯЙНОЪЙХЮЮКЦЛЗЕКВ\_Й  
ЮАЖШТЛ\_ЙУЭЕПБЮБЕШШВЙЪНЪОТКЧЦРКДМЛКЯПЧЭЗФЩНДЙНЭ  
ЫШЧВЦМЪВЦЭЭЕЛХЩЭЯЙТЮЗЧЮИДЙЧЮОККЛАЭЭЮБКЪЩЦБЛИТЗ  
ККЧОРИЧЙЭВЕХЕЖЦФЛМДЪК\_ЮИЦЮЦМКНЙФУЭОФЛПЙХХРЦЫНЛ  
ФЙУЭЩДВИЧЙШЮЦСЛБГПРЭАЪЕИТ\_ЩЭЗХЮГЧЧХЮЦЧРОБККДЧЙ  
ШВФЙП\_ЧЙЮДЪБККЛГТКОДБЦЕЦМКОЧОКЙЪЪРИТЙШВЦЭЭЕЛКЦЮЦ  
МРПЪЪКЪЙХККЧМЪПЖПБРЦФЛЗЦЛЮБИШКОЯХЙОТЙЩОИКШЛЩЦЭ  
ЩЦЦЩИДОЮЮЫЩЩЫВЗЪЮМГТАРЦШШЕЦЧЛОЯХЮЭЫШВИЯЙПЛЦФ  
ЩКМККОЧОЛЭГККЪДЪЩАЪЙЪЮГТКЪДРУБЧХУОТЙУТЦХЩХЧОУЭ  
ЪЩДХЛШРЦЙШВЦЫЭЛХХУЭГККЙЪЫЭВЦФЮФЪЪК\_БКПЕВТЫЮЦЪ  
ЛОЛКСЕЩКЦЭЕПЫВЫЙЩАБШМИХЦУЭЙОРНЭТНЮХЙЫВИТНШЛЙ  
ЩКЦЩЩЙДНКЯЧЪЕХГПКЕЦПРЭЫПНРОФРЭЙЪРОИЕЪЪЦТКРЪШСЕИ  
ЕКРЮХЕЭЯЙВЗЧЪЮИАЭК\_ЮИЦЭЩЩСГЯЙУЭБШВЮЫТКМДХРПЪХУ  
ЭЕШЫРНТНЭШКЪШОЧИЭЕШЪВНПШЕФЙЪРЫЕМЩЦТКЕЗФЮОЗЪНР  
ЦЪРНЪБХЕЦФЮФЪЪЛЭДЛЪЮИТЧОХЙХЭВШЦЛЫШЧРЦЧЛХЪЦЮЭБЗ  
МЛЩЧУЗЙЙАВБДФЭЫПШЩЦМЦЮЫТЧЕЖЙМШБЙНЭЖКТЧЪСПВЦЭЭ  
НДЦКЯСХКЛГЙЮЭЭКПНЯЧЪЗДНЦЭЗМЙЦЪЧШЕАКККЧЫУИЙЙЪЭГТЧ  
ЭЙНЦ\_ДЪУИЗИКМДЫЩЙЦЩЦВЛКЦЭЯЫХЮИЕКОЩТПВИПЦВ\_ЙЧВЭ  
ОЮЭЗШЪВЫЧУЙЯЙЪЛВПГЕАКЧЕЦЩРНЦДФЭАЙХЛВЭКЪЩЦЦОХЙЩ  
КЦШЭОИКНКДУКОДЪЩЗЧХРПГТФЭАШЫКЪЪКЪЖКНЕГЙЪЛЪХЛОЯХ  
ЪЦЫКЛЛШЭЛФЙЗПДЙЪНЯФЦЫНПШЕЪЙЮ\_ЪЪИЦШШЭГКЪЛВТШ  
ЮБШКВВЭКМЖПСКЪПК\_ЖПЧЪЦТКАЙЫЛНЗФУВЦЩЫЛАКТШЩШЭ  
ЙНЦ\_ДЪУИЦМЦЮЫТЧЕЖККЛЗЪЛПТЪЙЭЙШВЪШКЛИШМВЫКЭЩ  
ЦТКРЩПЫЕБЙРАДЙБПДЙТЮЦОЫРЪТЧЕЦОНРВИКОЩТПВИПЦЪВТКЪ  
ЪХЩЭГПКОИКШВИЙНЭЗКЧЛВЙПВБПКПДЪБЮЗЙЪЛЗХРЭДЛРБЧЙЙ\_Я  
ХУОТЙТВВХРЙЪЪКХВТЭЭЩЙЮОЧЯКЕЦЪЪЛЖК\_ЭЯЙЪШГЙХЮЕТЭЮ  
ГЙУОЕЪЛ\_ГТХЮЦЦЛИТАУЗЦХРПЦБРОИЧЛЪМКЭЕЦЧРЪЧМШЛЦЩЦ

ОИЭЪЕЩБУЖЦМКРБКШЩШШЕЦЧРЭИШЦЩАШКМЖТШЬБТКМЖП  
 ПИДРРКЯПК\_БКПЕВТЫЮЦЦЭЫКСВЦФЦЬБТЬЩЦПЧРЦМКАДЬЦ\_Г  
 ШЬПЯЙСВЖЪНЛЦКЭЩЦОЦЬЦЧРАДЙСЕЮЧУЫЦМЦЮЫТЧЕЖЙЩЯГИ  
 ЦЭЯЯКОЦМЦОИШЫАДЦКЕЦЩЦВЛКЦЭЫШЧЛ\_ЙЪНЯНЦПДМЦЬИЕЬ  
 ЪЦЭСВЦОЛ\_ГШКОВПЫЗЧХЦОТЙЩЦКЦШЭМЖКНЕБЙЬ\_ДПОЛЦЧЛБЬР  
 ШЛТЬШКПЬЪРХАЭК\_ЦЧРКЧЬЛБДМЦЭЗЙЬ\_ДПИЭИЪЦЖАШИЭЯЙЬЭЕ  
 ШПНДЛШШВЙЩЯЗЫЩЬИПЦЩГДЧЭГКХЮЮШЧЭЧЙПИХЙЬВШИК\_БХ  
 РИЦСЛИДРУПТЙЧЮБПШЩАТРЕЗКШЕЦМКЛЫЧЮЭБШВЮЫЕКЕЦШП  
 ЕГЙМВЮЙХРНПЫЮЦШЭМЖКНЕБЫЙЭЩЙСЮЫЪУКДЙХРЫККФЧЫЛ  
 ЭНПЫВЮЙП\_ЧЙПЛБРШЮЦЛЕИЧЙЪНЯП\_ЮИЕКЕЦЦЛНТИКАЧМЫЕБ  
 ШНКЧЙПЛЖШОЮЦЛЕИЧЙРЙЙТКЧФЩЙЧЙЛЭСПШЦМЬВЪШКБЩК  
 ПУЧЬЖЭВТШРИ

Для вычисления длинны ключа необходимо воспользоваться математической статистикой.

Для этого необходимо записать шифротекст в таблицу с  $n$  столбцами, где  $n$  определяется предполагаемой длиной ключа.

Предположим, что дина ключа лежит в диапазоне  $n \in [3; 6]$ .

Далее для каждой длинны ключа необходимо вычислить взаимное индексы совпадения в каждом столбце по формуле:

$$I_c(x) = \frac{\sum_{i=0}^{n-1} f_i(f_i - 1)}{m(m - 1)}$$

где:  $m$  – количество строк в столбце;  $f_i$  – частота повторения букв.

Далее показан расчет для  $n = 3$ :

В таблице 2.2 показана частота повторения букв алфавита в каждом столбце для ключа длиной 3 символов.

Таблица 2.2 – Частота повторения букв в столбце для  $n = 3$

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_
7	20	23	10	14	25	13	16	27	45	46	39	9	17	18	29	21	3	27	14	11	21	30	29	39	36	13	17	29	39	25	15	11
12	20	25	8	19	26	13	12	19	44	55	26	14	21	20	23	18	5	19	11	9	25	54	23	30	27	11	28	36	32	26	15	11
10	19	17	11	17	22	3	14	23	48	51	36	20	16	17	30	24	9	20	12	10	22	42	35	26	29	16	18	29	44	23	12	12

Расчет взаимного индекса совпадения для 1-го столбца:

$$I_c(x) = \frac{7 \cdot 6 + 20 \cdot 19 + 23 \cdot 22 + 10 \cdot 9 + 14 \cdot 13 + 25 \cdot 24 + 13 \cdot 12 + 16 \cdot 15 + 27 \cdot 26 + 45 \cdot 44 + 46 \cdot 45 + 39 \cdot 38 + 9 \cdot 8 + 17 \cdot 16 + 18 \cdot 17 + 29 \cdot 28 + 21 \cdot 20 + 3 \cdot 2 + 27 \cdot 26 + 14 \cdot 13 + 11 \cdot 10 + 21 \cdot 20 + 30 \cdot 29 + 29 \cdot 28 + 39 \cdot 38 + 36 \cdot 35 + 13 \cdot 12 + 17 \cdot 16 + 29 \cdot 28 + 39 \cdot 38 + 25 \cdot 24 + 15 \cdot 14 + 11 \cdot 10}{738 \cdot 737} = 0,0364$$

Расчет взаимного индекса совпадения для 2-го столбца:

$$I_c(x) = \frac{12 \cdot 11 + 20 \cdot 19 + 25 \cdot 24 + 8 \cdot 7 + 19 \cdot 18 + 26 \cdot 25 + 13 \cdot 12 + 12 \cdot 11 + 19 \cdot 18 + 44 \cdot 43 + 55 \cdot 54 + 26 \cdot 25 + 14 \cdot 13 + 21 \cdot 20 + 20 \cdot 19 + 23 \cdot 22 + 18 \cdot 17 + 5 \cdot 4 + 19 \cdot 18 + 11 \cdot 10 + 9 \cdot 8 + 25 \cdot 24 + 54 \cdot 53 + 23 \cdot 22 + 30 \cdot 29 + 27 \cdot 26 + 11 \cdot 10 + 28 \cdot 27 + 36 \cdot 35 + 32 \cdot 31 + 26 \cdot 25 + 15 \cdot 14 + 11 \cdot 10}{737 \cdot 736} = 0,03737$$

Расчет взаимного индекса совпадения для 3-го столбца:

$$I_c(x) = \frac{10 \cdot 9 + 19 \cdot 18 + 17 \cdot 16 + 11 \cdot 10 + 17 \cdot 16 + 22 \cdot 21 + 1 + 3 \cdot 2 + 14 \cdot 13 + 23 \cdot 22 + 48 \cdot 47 + 51 \cdot 50 + 36 \cdot 35 + 20 \cdot 19 + 16 \cdot 15 + 17 \cdot 16 + 30 \cdot 29 + 24 \cdot 23 + 9 \cdot 8 + 20 \cdot 19 + 12 \cdot 11 + 10 \cdot 9 + 22 \cdot 21 + 42 \cdot 41 + 35 \cdot 34 + 26 \cdot 25 + 29 \cdot 28 + 16 \cdot 15 + 18 \cdot 17 + 29 \cdot 28 + 44 \cdot 43 + 23 \cdot 22 + 12 \cdot 11 + 12 \cdot 11}{737 \cdot 736} = 0,03715$$

Далее показан расчет для  $n = 4$ :

В таблице 2.3 показана частота повторения букв алфавита в каждом столбце для ключа длиной 3 символа.

Таблица 2.3 – Частота повторения букв в столбце для  $n = 4$

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_		
2	6	1	1	5	14	0	3	9	10	2	45	10	22	5	13	4	1	8	6	40	2	16	35	11	25	48	10	20	16	22	12	0	2	1
2	5	5	1	0	7	5	1	4	8	8	3	40	8	23	2	21	33	9	11	33	3	16	27	21	32	50	12	21	26	21	20	0	3	
11	18	40	3	4	40	4	9	29	10	24	43	9	17	36	20	22	0	1	2	4	8	2	1	12	13	0	4	11	78	46	6	26		
14	30	19	24	41	12	20	29	27	17	0	8	4	9	4	0	0	2	14	0	7	9	86	40	3	19	8	22	35	4	8	34	4		

Расчет взаимного индекса совпадения для 1-го столбца:

$$I_c(x) = \frac{2 \cdot 1 + 6 \cdot 5 + 1 \cdot 0 + 1 \cdot 0 + 5 \cdot 4 + 14 \cdot 13 + 3 \cdot 2 + 9 \cdot 8 + 102 \cdot 101 + 45 \cdot 44 + 10 \cdot 9 + 22 \cdot 21 + 5 \cdot 4 + 13 \cdot 12 + 41 \cdot 40 + 8 \cdot 7 + 6 \cdot 5 + 40 \cdot 39 + 2 \cdot 1 + 16 \cdot 15 + 35 \cdot 34 + 11 \cdot 10 + 25 \cdot 24 + 48 \cdot 47 + 10 \cdot 9 + 20 \cdot 19 + 16 \cdot 15 + 22 \cdot 21 + 12 \cdot 11 + 0 \cdot (-1) + 2 \cdot 1 + 1 \cdot 0}{553 \cdot 552}$$

$$= 0,07309$$

Расчет взаимного индекса совпадения для 2-го столбца:

$$I_c(x) = \frac{5 \cdot 4 + 5 \cdot 4 + 1 \cdot 0 + 0 \cdot (-1) + 7 \cdot 6 + 5 \cdot 4 + 1 \cdot 0 + 4 \cdot 3 + 8 \cdot 7 + 83 \cdot 82 + 40 \cdot 39 + 8 \cdot 7 + 23 \cdot 22 + 2 \cdot 1 + 21 \cdot 20 + 33 \cdot 32 + 9 \cdot 8 + 11 \cdot 10 + 33 \cdot 32 + 3 \cdot 2 + 16 \cdot 15 + 27 \cdot 26 + 21 \cdot 20 + 32 \cdot 31 + 50 \cdot 49 + 12 \cdot 11 + 21 \cdot 20 + 26 \cdot 25 + 21 \cdot 20 + 20 \cdot 19 + 0 \cdot (-1) + 3 \cdot 2}{553 \cdot 552}$$

$$= 0,06104$$

Расчет взаимного индекса совпадения для 3-го столбца:

$$I_c(x) = \frac{11 \cdot 10 + 18 \cdot 17 + 40 \cdot 39 + 3 \cdot 2 + 4 \cdot 3 + 40 \cdot 39 + 4 \cdot 3 + 9 \cdot 8 + 29 \cdot 28 + 10 \cdot 9 + 24 \cdot 23 + 43 \cdot 42 + 9 \cdot 8 + 17 \cdot 16 + 36 \cdot 35 + 20 \cdot 19 + 22 \cdot 21 + 0 \cdot (-1) + 1 \cdot 0 + 2 \cdot 1 + 4 \cdot 3 + 8 \cdot 7 + 2 \cdot 1 + 1 \cdot 0 + 12 \cdot 11 + 13 \cdot 12 + 0 \cdot (-1) + 4 \cdot 3 + 11 \cdot 10 + 78 \cdot 77 + 46 \cdot 45 + 6 \cdot 5 + 26 \cdot 25}{553 \cdot 552}$$

$$= 0,06087$$

Расчет взаимного индекса совпадения для 4-го столбца:

$$I_c(x) = \frac{14 \cdot 13 + 30 \cdot 29 + 19 \cdot 18 + 24 \cdot 23 + 41 \cdot 40 + 12 \cdot 11 + 20 \cdot 19 + 29 \cdot 28 + 27 \cdot 26 + 17 \cdot 16 + 0 \cdot (-1) + 8 \cdot 7 + 4 \cdot 3 + 9 \cdot 8 + 4 \cdot 3 + 0 \cdot (-1) + 0 \cdot (-1) + 2 \cdot 1 + 14 \cdot 13 + 0 \cdot (-1) + 7 \cdot 6 + 9 \cdot 8 + 86 \cdot 85 + 40 \cdot 39 + 3 \cdot 2 + 19 \cdot 18 + 8 \cdot 7 + 22 \cdot 21 + 35 \cdot 34 + 4 \cdot 3 + 4 \cdot 3 + 8 \cdot 7 + 34 \cdot 33 + 4 \cdot 3}{553 \cdot 552}$$

$$= 0,06048$$

В таблице 2.4 показана частота повторения букв алфавита в каждом столбце для ключа длиной 5 символа.

Таблица 2.4 – Частота повторения букв в столбце для  $n = 5$

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_
5	15	10	8	9	19	5	13	15	23	38	24	6	10	11	25	6	3	13	6	6	12	23	14	13	25	10	8	15	23	12	14	4
7	7	9	7	12	17	7	9	13	25	32	15	11	15	9	24	13	2	16	5	5	17	23	18	23	22	6	11	15	18	16	6	8
4	11	12	5	13	13	5	6	14	33	21	17	11	12	12	12	14	3	10	8	8	13	23	23	24	15	8	19	22	22	13	9	7
6	16	15	3	7	14	6	8	16	28	28	27	5	8	11	7	15	5	13	7	7	14	31	15	15	19	8	16	24	19	15	5	9
7	10	19	6	9	10	6	6	11	28	33	18	10	9	12	14	15	4	14	11	4	12	26	17	20	11	8	9	18	33	18	8	6

Расчет взаимного индекса совпадения для 1-го столбца:

$$I_c(x) = 0,038232$$

Расчет взаимного индекса совпадения для 2-го столбца:

$$I_c(x) = 0,036209$$

Расчет взаимного индекса совпадения для 3-го столбца:

$$I_c(x) = 0,03583$$

Расчет взаимного индекса совпадения для 4-го столбца:

$$I_c(x) = 0,037523$$

Расчет взаимного индекса совпадения для 5-го столбца:

$$I_c(x) = 0,037872$$

В таблице 2.5 показана частота повторения букв алфавита в каждом столбце для ключа длиной 6 символов.

Таблица 2.5 – Частота повторения букв в столбце для  $n = 6$

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_
2	11	16	2	1	17	2	2	19	38	15	21	7	6	16	22	10	0	16	1	9	14	4	8	26	5	5	4	10	28	18	4	10
7	12	9	8	13	5	11	7	11	10	28	9	4	10	2	5	11	4	7	9	3	9	48	17	9	19	4	19	21	7	16	11	4
6	5	9	2	2	16	0	5	11	40	27	15	14	5	15	21	13	5	13	1	5	13	3	12	13	10	8	7	8	37	18	0	10
5	9	7	8	13	8	11	14	8	7	31	18	2	11	2	7	11	3	11	13	2	7	26	21	13	31	8	13	19	11	7	11	1
5	8	16	0	6	21	2	5	8	34	27	17	10	11	18	18	7	1	12	2	6	16	6	6	21	8	7	9	15	25	10	4	7
4	14	8	9	15	6	3	9	12	8	24	21	6	11	2	9	11	4	7	11	5	9	39	23	13	19	8	11	21	7	5	12	2

Расчет взаимного индекса совпадения для 1-го столбца:

$$I_c(x) = 0,047057$$

Расчет взаимного индекса совпадения для 2-го столбца:

$$I_c(x) = 0,045776$$

Расчет взаимного индекса совпадения для 3-го столбца:

$$I_c(x) = 0,048412$$

Расчет взаимного индекса совпадения для 4-го столбца:

$$I_c(x) = 0,041107$$

Расчет взаимного индекса совпадения для 5-го столбца:

$$I_c(x) = 0,037872$$

Расчет взаимного индекса совпадения для 6-го столбца:

$$I_c(x) = 0,04182$$

Так как взаимный индекс совпадения значения для символов русского языка должен находиться в пределах 0,053 - 0,07 то можно сделать вывод что длина ключа 4 символа.

Так как известно, что длина ключа составляет 4 символа, то для вычисления ключевого слова необходимо зашифрованный текст представить в виде таблицы, состоящей из 4 столбцов (таблица 2.6).

Таблица 2.6 – Преобразование шифротекста в таблицу по 4 символа

Y1	Y2	Y3	Y4
Щ	Щ	Б	Ч
Х	У	Э	Й
Р	У	К	Ч
Ь	Ж	Э	З
П	Ы	Б	М
П	К	В	Ь
Й	Ь	Е	Б
Е	Ш	Л	Ц
С	Л	Я	Я
Х	Щ	О	Т
Й	П	Н	Д
Р	Л	Ц	Я
Ц	К	А	Д
Х	Щ	О	Д
Ц	К	Л	Ш
Г	Й	-	Я
Х	Л	Э	Д
Ч	Л	Э	Н
Ь	Щ	Э	Ь



Y1	Y2	Y3	Y4
У	К	Р	Э
Т	Ш	Ю	И
Е	К	К	Ь
Й	–	Л	Н
П	Э	О	Х
Й	У	Э	З
Ь	Л	И	Ч
Й	Ъ	Н	Д
В	Л	П	Т
Ы	Й	Э	З
Й	Щ	П	М
Ш	Ч	Э	Я
Й	Ч	Ю	И
П	Ы	Щ	Ф
Й	Щ	К	Я
Й	Р	В	Ц
Щ	Щ	У	Ь
Х	Щ	–	Ч
Х	У	Э	Я
Й	Ъ	Л	Ц
Ш	М	Ш	А
Ч	Щ	–	Ь
Ч	У	Ы	Ц
Л	Ц	Ю	Ъ
Ш	Ь	И	Д
М	У	И	Я
Й	Щ	К	Ч
Й	Б	Р	И
Е	К	К	Ь
Й	Т	Ю	Е
Х	Л	З	Ч
Х	Л	Э	Е
Ъ	У	Х	Ь
Х	К	–	Ц
Ы	Н	Л	Ф
Й	Х	Л	В
Ч	Л	П	Й
Й	Щ	К	Ч
Й	Х	Е	Г
Э	Ц	Ю	З
Е	К	–	Ц
Ф	Ы	В	З
Х	Л	Э	Я
Й	Т	Ю	Б
Т	Ц	Ю	З
Е	К	О	Б
П	Т	Ю	В

Y1	Y2	Y3	Y4
Т	К	Б	Ь
М	Ю	Х	А
К	К	Р	Ъ
Ш	Н	Ю	Ж
Т	Н	Ю	Б
К	К	В	Ь
Й	Ю	О	Е
Ш	Х	Л	Я
Ь	Ж	О	Х
Й	У	Э	Д
Л	Щ	Б	Ж
Т	Э	Щ	З
И	К	–	З
П	К	Я	С
Х	Щ	Э	Ъ
Ш	Э	Л	Щ
Ш	К	Ф	Ь
Ъ	Р	Д	Ц
Щ	Щ	И	Н
К	Ь	Ю	Ц
Ц	Л	Х	Ч
Й	П	Л	Б
Р	Ш	Ю	Ц
Л	Е	И	Ч
Й	Ш	Ю	Щ
Ы	Р	А	Ы
К	К	Л	З
Ь	Л	–	Я
Ь	Ж	Э	Ж
Ш	П	Е	И
П	Ц	Щ	З
Ф	У	Ж	Ц
О	Щ	Й	Ц
Ы	Н	Л	Ф
Й	Х	Л	В
Ч	Л	П	Й
Й	Э	Е	Л
Э	И	Э	Ы
П	Н	Е	Н
П	Ь	З	Й
З	К	Г	Я
С	Ш	Щ	Ц
Ч	Л	Э	Ы
М	Щ	Н	Ь
Й	М	Ш	Б
К	К	Й	Ь
Ь	Р	И	Т

Y1	Y2	Y3	Y4
Й	Н	В	И
П	Ы	Э	Щ
Д	Ц	Э	З
Ь	Л	_	Г
Т	К	П	Ж
И	Ь	И	Я
Ы	Ж	Э	Я
Й	Ь	П	Й
А	Л	И	Я
Й	Н	О	Ь
Й	Х	Ю	Ю
К	Ц	Л	З
Е	К	В	_
Й	Ю	А	Ж
Ш	Т	Л	_
Й	У	Э	Е
П	Б	Ю	Б
Е	Ш	Ш	В
Й	Ь	Н	Ь
О	Т	К	Ч
Ц	Р	К	Д
М	Л	К	Я
П	Ч	Э	З
Ф	Щ	Н	Д
Й	Н	Э	Ы
Ш	Ч	В	Ц
М	Ь	В	Ц
Э	Э	Е	Л
Х	Щ	Э	Я
Й	Т	Ю	З
Ч	Ю	И	Д
Й	Ч	Ю	О
К	К	Л	А
Э	Э	Ю	Б
К	Ь	Щ	Ц
Б	Л	И	Т
З	К	К	Ч
О	Р	И	Ч
Й	Э	В	Е
Х	Е	Ж	Ц
Ф	Л	М	Д
Ь	К	_	Ю
И	Ц	Ю	Ц
М	К	Н	Й
Ф	У	Э	О
Ф	Л	П	Й
Х	Х	Р	Ц

Y1	Y2	Y3	Y4
Ы	Н	Л	Ф
Й	У	Э	Щ
Д	В	И	Ч
Й	Ш	Ю	Ц
С	Л	Б	Г
П	Р	Э	А
Ъ	Е	И	Т
_	Щ	Э	З
Х	Ю	Г	Ч
Ч	Х	Ю	Ц
Ч	Р	О	Б
К	К	Д	Ч
Й	Ш	В	Ф
Й	П	_	Ч
Й	Ю	Д	Б
К	К	Л	Г
Т	К	О	Д
Б	Ц	Е	Ц
М	К	О	Ч
О	К	Й	Ь
Ь	Р	И	Т
Й	Ш	В	Ц
Э	Э	Е	Л
К	Ц	Ю	Ц
М	Р	П	Ь
Ъ	К	Б	Й
Х	К	К	Ч
М	Ь	П	Ж
П	Б	Р	Ц
Ф	Л	З	Ц
Л	Ю	Б	И
Ш	К	О	Я
Х	Й	О	Т
Й	Щ	О	И
К	Ш	Л	Щ
Т	Э	Щ	Ц
Ц	Щ	И	Д
О	Ю	Ы	Ц
Щ	Ы	В	З
Ь	Ю	М	Г
Т	А	Р	Ц
Ш	Ш	Е	Ц
Ч	Л	О	Я
Х	Ю	Э	Ы
Ш	В	И	Я
Й	П	Л	Ц
Ф	Щ	К	М

Y1	Y2	Y3	Y4
К	К	О	Ч
О	Л	Э	Г
К	К	Б	Д
Ъ	Щ	А	Ь
Й	Ь	Ю	Г
Т	К	Б	Д
Р	У	Б	Ч
Х	У	О	Т
Й	У	Т	Ц
Х	Щ	Х	Ч
О	У	Э	Е
Ъ	Щ	Д	Х
Л	Ш	Р	Щ
Й	Ш	В	Ц
Ы	Э	Л	Х
Х	У	Э	Г
К	К	Й	Ь
Ы	Э	В	Ц
Ф	Ю	Ф	Ь
Ъ	К	–	Б
К	П	Е	В
Т	Ы	Ю	Ц
Ъ	Л	О	Л
К	С	Е	Щ
К	Ц	Э	Е
П	Ы	В	Ы
Й	Щ	А	Б
Ш	М	И	Х
Ц	У	Э	Й
О	Р	Н	Э
Т	Н	Ю	Х
Й	Ы	В	И
Т	Н	Ш	Л
Й	Щ	К	Ц
Щ	Щ	Й	Д
Н	К	Я	Ч
Ъ	Е	Х	Г
П	К	Е	Ц
П	Р	Э	Ы
П	Н	Р	О
Ф	Р	Э	Й
Ы	Р	О	И
Е	Ь	Ь	Ц
Т	К	Р	Б
Ш	С	Е	И
Е	К	Р	Ю
Х	Е	Э	Я

Y1	Y2	Y3	Y4
Й	В	З	Ч
Ь	Ю	И	А
Э	К	–	Ю
И	Ц	Э	Щ
Ш	С	Г	Я
Й	У	Э	Б
Ш	В	Ю	Ы
Т	К	М	Д
Х	Р	П	Ь
Х	У	Э	Е
Ш	Ы	Р	Н
Т	Н	Э	Ш
К	Ы	Ш	О
Ч	И	Э	Е
Ш	Ь	В	Н
П	Ш	Е	Ф
Й	Ь	Р	Ы
Е	М	Ш	Ц
Т	К	Е	З
Ф	Ю	О	З
Ь	Н	Р	Ц
Ь	Р	Н	Ь
Б	Х	Е	Ц
Ф	Ю	Ф	Ь
Ъ	Л	Э	Д
Л	Ы	Ю	И
Т	Ч	О	Х
Й	Х	Э	В
Ш	Ц	Л	Ы
Ш	Ч	Р	Ц
Ч	Л	Х	Ь
Ц	Ю	Э	Б
З	М	Л	Щ
Ч	У	З	Й
Й	А	В	Б
Д	Ф	Э	Ы
П	Ш	Щ	Ц
М	Ц	Ю	Ы
Т	Ч	Е	Ж
Й	М	Ш	Б
Й	Н	Э	Ж
К	Т	Ч	Ь
С	П	В	Ц
Э	Э	Н	Д
Ц	К	Я	С
Х	К	Л	Г
Й	Ю	Э	Э

У1	У2	У3	У4
К	П	Н	Я
Ч	Ь	З	Д
Н	Щ	Э	З
М	Й	Ц	Ь
Ч	Ш	Е	А
К	К	К	Ч
Ы	У	И	Й
Й	Ь	Э	Г
Т	Ч	Э	Й
Н	Щ	–	Д
Ъ	У	И	З
И	К	М	Д
Ь	Щ	Й	Ц
Щ	Щ	В	Л
К	Ц	Э	Я
Ы	Х	Ю	И
Е	К	О	Щ
Т	П	В	И
П	Ц	В	–
Й	Ч	В	Э
О	Ю	Э	З
Ш	Ь	В	Ы
Ч	У	Й	Я
Й	Ъ	Л	В
П	Г	Е	А
К	Ч	Е	Ц
Щ	Р	Н	Щ
Д	Ф	Э	А
Й	Х	Л	В
Э	К	Ь	Щ
Т	Ц	О	Х
Й	Щ	К	Ц
Ш	Э	О	И
К	Н	К	Д
У	К	О	Д
Ъ	Щ	З	Ч
Х	Р	П	Г
Т	Ф	Э	А
Ш	Ы	К	Ь
Ь	К	Б	Ж
К	Н	Е	Г
Й	Ь	Л	Ъ
Х	Л	О	Я
Х	Ь	Ь	Ц
Ы	К	Л	Л
Ш	Э	Л	Ф
Й	З	П	Д

У1	У2	У3	У4
Й	Ъ	Н	Я
Ф	Ц	Ы	Н
П	Ш	Е	Ь
Й	Ю	–	Ь
Ъ	Й	И	Ц
Ш	Ш	Э	Г
К	Ъ	Л	В
Т	Ш	Ю	Б
Ш	К	В	В
Э	К	М	Ж
П	С	К	Ь
П	К	–	Ж
П	Ч	Ь	Ц
Т	К	А	Й
Ы	Л	Н	З
Ф	У	В	Ц
Щ	Ы	Л	А
К	Т	Ш	Ц
Ш	Ш	Э	Й
Н	Щ	–	Д
Ъ	У	И	Ц
М	Ц	Ю	Ы
Т	Ч	Е	Ж
К	К	Л	З
Ь	Л	П	Т
Ы	Й	Э	Й
Й	Ш	В	Ъ
Ш	К	Л	И
Ш	М	В	Ы
К	Э	Щ	Ц
Т	К	Р	Щ
П	Ы	Е	Б
Й	Р	А	Д
Й	Б	П	Д
Й	Т	Ю	Ц
О	Ы	Р	Ъ
Т	Ч	Е	Ц
О	Н	Р	В
И	К	О	Щ
Т	П	В	И
П	Ц	Ь	В
Т	К	Б	Ь
Х	Щ	Э	Г
П	К	О	И
К	Ш	В	И
Й	Н	Э	З
К	Ч	Л	В



Y1	Y2	Y3	Y4
Й	П	В	Б
П	К	П	Д
Ь	Б	Ю	З
Й	Ъ	Л	З
Х	Р	Э	Д
Л	Р	Б	Ч
Й	Й	–	Я
Х	У	О	Т
Й	Т	В	В
Х	Р	Й	Ь
Ъ	К	Х	В
Т	Э	Э	Щ
Й	Ю	О	Ч
Я	К	Е	Ц
Б	Ъ	Л	Ж
К	–	Э	Я
Й	Ь	Ш	Г
Й	Х	Ю	Е
Т	Э	Ю	Г
Й	У	О	Е
Ъ	Л	–	Г
Т	Х	Ю	Ц
Ц	Л	И	Т
А	У	З	Ц
Х	Р	П	Ц
Б	Р	О	И
Ч	Л	Б	М
К	Э	Е	Ц
Ч	Р	Б	Ч
М	Ш	Л	Ц
Щ	Щ	О	И
Э	Ъ	Е	Щ
Б	У	Ж	Ц
М	К	Р	Б
К	Ш	Ш	Ц
Ш	Ш	Е	Ц
Ч	Р	Э	И
Ш	Ц	Щ	А
Ш	К	М	Ж
Т	Ш	Ь	Б
Т	К	М	Ж
П	П	И	Д
Р	Р	К	Я
П	К	–	Б
К	П	Е	В
Т	Ы	Ю	Ц
Ч	Щ	Э	Ы

У1	У2	У3	У4
К	С	В	Ц
Ф	Ц	Ь	Б
Т	Ь	Щ	Ц
П	Ч	Р	Ц
М	К	А	Д
Ь	Щ	_	Г
Ш	Ь	П	Я
Й	С	В	Ж
Ь	Н	Л	Щ
К	Э	Щ	Ц
О	Ц	Ь	Ц
Ч	Р	А	Д
Й	С	Е	Ю
Ч	У	Ы	Ц
М	Ц	Ю	Ы
Т	Ч	Е	Ж
Й	Щ	Я	Г
И	Ц	Э	Я
Я	К	О	Ц
М	Щ	О	И
Ш	Ы	А	Д
Ц	К	Е	Ц
Щ	Щ	В	Л
К	Ц	Э	Ы
Ш	Ч	Л	_
Й	Ь	Н	Я
Н	Щ	П	Д
М	Ц	Ь	И
Е	Ь	Ь	Ц
Э	С	В	Ц
О	Л	_	Г
Ш	К	О	В
П	Ы	З	Ч
Х	Щ	О	Т
Й	Щ	К	Ц
Ш	Э	М	Ж
К	Н	Е	Б
Й	Ь	_	Д
П	О	Л	Ц
Ч	Л	Б	Ь
Р	Ш	Л	Ь
Ш	К	П	Ь
Ъ	Р	Х	А
Э	К	_	Ц
Ч	Р	К	Ч
Ъ	Л	Б	Д
М	Щ	Э	З

У1	У2	У3	У4
Й	Ь	–	Д
П	И	Э	И
Ъ	Щ	Ж	А
Ш	И	Э	Я
Й	Ь	Э	Е
Ш	П	Н	Д
Л	Ш	Ш	В
Й	Щ	Я	З
Ь	Щ	Ь	И
П	Ц	Щ	Г
Д	Ч	Э	Г
К	Х	Ю	Ю
Ш	Ч	Э	Ч
Й	П	И	Х
Й	Ь	В	Ш
И	К	–	Ь
Х	Р	И	Ц
С	Л	И	Д
Р	У	П	Т
Й	Ч	Ю	Б
П	Ш	Щ	А
Т	Р	Э	З
К	Ш	Е	Ц
М	К	Л	Ы
Ч	Ю	Э	Б
Ш	В	Ю	Ы
Е	К	Е	Ц
Ш	П	Е	Г
Й	М	В	Ю
Й	Х	Р	Н
П	Ы	Ю	Ц
Ш	Э	М	Ж
К	Н	Е	Б
Ы	Й	Э	Щ
Й	С	Ю	Ы
Ъ	У	К	Д
Й	Х	Р	Ы
К	К	Ф	Ч
Ы	Л	Э	Н
П	Ы	В	Ю
Й	П	–	Ч
Й	П	Л	Б
Р	Ш	Ю	Ц
Л	Е	И	Ч
Й	Ъ	Н	Я
П	–	Ю	И
Е	К	Е	Ц

Y1	Y2	Y3	Y4
Ц	Л	Н	Т
И	К	А	Ч
М	Ы	Е	Б
Ш	Н	К	Ч
Й	П	Л	Ж
Ш	О	Ю	Ц
Л	Е	И	Ч
Й	Р	Й	Й
Й	Т	К	Ч
Ф	Щ	Й	Ч
Й	Л	Э	Ь
С	П	Ш	Ц
М	Ь	В	Ъ
Ш	К	Б	Щ
К	П	У	Ч
Ь	Ж	Э	В
Т	Ш	Р	И

Для нахождения ключевого слова можно использовать так называемый взаимный индекс совпадения, который вычисляется по формуле:

$$MI_C(x, y) = \frac{\sum_{i=0}^{n-1} f_i \cdot f_i^1}{m \cdot m^1}$$

где:  $f_i, f_i^1$  – частота буквы  $i$  в столбцах  $Y_i$  и  $Y_i^1$  соответственно;  $m, m^1$  количество букв в столбцах  $Y_i$  и  $Y_i^1$  соответственно.

Так как каждый из столбцов таблицы является результатом шифрования фрагмента открытого текста простой заменой, определяемой подстановкой, то необходимо провести оценку взаимных индексов совпадения.

Тогда для таблицы частот букв русского языка (таблица 2.3) взаимный индекс совпадения равен:

– для столбцов 1, 2:

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	_		
2	6	1	1	5	14	0	3	9	10	2	45	10	22	5	13	4	1	8	6	40	2	16	35	11	25	48	10	20	16	22	12	0	2	1
2	5	5	1	0	7	5	1	4	8	8	3	40	8	23	2	21	33	9	11	33	3	16	27	21	32	50	12	21	26	21	20	0	3	
11	18	40	3	4	40	4	9	29	10	24	43	9	17	36	20	22	0	1	2	4	8	2	1	12	13	0	4	11	78	46	6	26		
14	30	19	24	41	12	20	29	27	17	0	8	4	9	4	0	0	2	14	0	7	9	86	40	3	19	8	22	35	4	8	34	4		

$$MI_C(x, y) = \frac{2 \cdot 2 + 6 \cdot 5 + 1 \cdot 5 + 1 \cdot 1 + 5 \cdot 0 + 14 \cdot 7 + 0 \cdot 4 + 3 \cdot 1 + 9 \cdot 4 + 100 \cdot 8 +}{553 \cdot 553}$$

$$\frac{44 \cdot 82 + 10 \cdot 39 + 21 \cdot 8 + 5 \cdot 23 + 13 \cdot 2 + 41 \cdot 19 + 8 \cdot 33 + 5 \cdot 9 + 39 \cdot 10 + 2 \cdot 33 + 15 \cdot 3 + 35 \cdot 16 + 11 \cdot 27 + 25 \cdot 21 + 47 \cdot 31 + 10 \cdot 49 + 20 \cdot 12 + 16 \cdot 21 + 21 \cdot 25 + 12 \cdot 21 + 0 \cdot 20 + 2 \cdot 0 + 1 \cdot 3}{553 \cdot 553} = 0,03779$$

– для столбцов 2, 3:

$$MI_C(x, y) = \frac{2 \cdot 11 + 5 \cdot 17 + 5 \cdot 39 + 1 \cdot 3 + 0 \cdot 4 + 7 \cdot 40 + 4 \cdot 4 + 1 \cdot 9 + 4 \cdot 29 + 8 \cdot 9 + 82 \cdot 23 + 39 \cdot 43 + 8 \cdot 9 + 23 \cdot 17 + 2 \cdot 36 + 19 \cdot 20 + 33 \cdot 21 + 9 \cdot 0 + 10 \cdot 1 + 33 \cdot 1 + 3 \cdot 4 + 16 \cdot 8 + 27 \cdot 2 + 21 \cdot 1 + 31 \cdot 11 + 49 \cdot 13 + 12 \cdot 0 + 21 \cdot 4 + 25 \cdot 11 + 21 \cdot 76 + 20 \cdot 46 + 0 \cdot 6 + 3 \cdot 26}{549 \cdot 549} = 0,03322$$

– для столбцов 3, 4:

$$MI_C(x, y) = \frac{11 \cdot 14 + 17 \cdot 30 + 39 \cdot 18 + 3 \cdot 24 + 4 \cdot 41 + 40 \cdot 12 + 4 \cdot 20 + 9 \cdot 29 + 29 \cdot 26 + 9 \cdot 17 + 23 \cdot 0 + 43 \cdot 8 + 9 \cdot 4 + 17 \cdot 9 + 36 \cdot 4 + 20 \cdot 0 + 21 \cdot 0 + 0 \cdot 2 + 1 \cdot 14 + 1 \cdot 0 + 4 \cdot 7 + 8 \cdot 9 + 2 \cdot 85 + 1 \cdot 37 + 11 \cdot 3 + 13 \cdot 18 + 0 \cdot 7 + 4 \cdot 22 + 11 \cdot 34 + 76 \cdot 4 + 46 \cdot 8 + 6 \cdot 34 + 26 \cdot 4}{553 \cdot 553} = 0,01974$$

Так как для ключевого слова взаимный индекс совпадения для алфавита русского языка должен находиться в пределах 0,053 – 0,07 то необходимо произвести сдвиги в столбцах 2, 3, 4 относительно столбца 1.

Тогда сдвинув столбец 2 на 1, столбец 3 на 20 и столбец 4 на 13 получим отношение частот букв между столбцами (таблица 2.7)

Таблица 2.7 – Сдвинутые значения частот символов

2	6	1	1	5	14	0	0	3	9	100	44	10	21	5	13	41	8	5	39	2	15	35	11	25	47	10	20	16	21	12	0	2	1
5	5	1	0	7	0	4	1	4	8	82	39	8	23	2	19	33	9	10	33	3	16	27	21	31	49	12	21	25	21	20	0	3	2
1	4	8	2	1	11	13	0	4	11	76	46	6	26	11	17	39	3	4	40	0	4	9	29	9	23	43	9	17	36	20	21	0	1
4	9	4	0	0	2	14	0	7	9	85	37	3	18	7	22	34	4	8	34	4	14	30	18	24	41	12	0	20	29	26	17	0	8

После сдвига взаимный индекс совпадения равен:

– для столбцов 1,2:

$$MI_C(x, y) = 0,064704$$

– для столбцов 2,3:

$$MI_C(x, y) = 0,053945$$

– для столбцов 3, 4:

$$MI_C(x, y) = 0,055669$$

Полученные индексы совпадения соответствуют условию нахождения индекса совпадения в пределах 0,053 – 0,07.

Тогда сдвинув значение алфавита относительно первого столбца на 1, 20 и 13 получим (таблица 2.8).

Таблица 2.8 – Сдвинутые значения алфавита

№ п/п	Y1	Y2	Y3	Y4
1.	А	Б	У	М
2.	Б	В	Ф	Н
3.	В	Г	Х	О
4.	Г	Д	Ц	П
5.	Д	Е	Ч	Р
6.	Е	Ё	Ш	С
7.	Ё	Ж	Щ	Т
8.	Ж	З	Ъ	У
9.	З	И	Ы	Ф
10.	И	Й	Ь	Х
11.	Й	К	Э	Ц
12.	К	Л	Ю	Ч
13.	Л	М	Я	Ш
14.	М	Н	–	Щ
15.	Н	О	А	Ъ
16.	О	П	Б	Ы
17.	П	Р	В	Ь
18.	Р	С	Г	Э
19.	С	Т	Д	Ю
20.	Т	У	Е	Я
21.	У	Ф	Ё	–
22.	Ф	Х	Ж	А
23.	Х	Ц	З	Б
24.	Ц	Ч	И	В
25.	Ч	Ш	Й	Г

№ п/п	Y1	Y2	Y3	Y4
26.	Ш	Щ	К	Д
27.	Щ	Ъ	Л	Е
28.	Ъ	Ы	М	Ё
29.	Ы	Ь	Н	Ж
30.	Ь	Э	О	З
31.	Э	Ю	П	И
32.	Ю	Я	Р	Й
33.	Я	–	С	К
34.	–	А	Т	Л
35.	А	Б	У	М

Из таблицы 2.8 видно, что ключевое слово представлено в строке 12 и его значение «КЛЮЧ».

### Указания по технике безопасности

В начале каждого семестра, со студентами должен проводиться инструктаж по технике безопасности в лаборатории. Во время нахождения студента в лаборатории и выполнения лабораторных работ студент не должен нарушать инструкции по охране труда с персональным компьютером ИОТ-37-ИВЛ-19, и инструкцию о мерах пожарной безопасности ИБП-01-2016.

### Методические указания к выполнению работы

Каждому студенту необходимо расшифровать закодированный текст шифром Виженера в соответствии с вариантом (таблица 2.9). Известно, что длина ключа 4 символа.

При выполнении работы разрешается использовать любые технические и программные средства.

Таблица 2.9 – Задания для выполнения работы

Вариант	Задание
1.	БРНАЕЗСМФСЮЖУФЫГЪБТЙУБЪГБАНРВБЪГЕФЫЮБВНИВФЪОВОНАВЙРЦМ ВЛРЕАНКДВДЛПЗНБВФЦХЪУШЖЪБПЯМПЦЮЕКЪЛВДОЮАРЯЕФИОУБЯРВ АНЛХБЯГЮБСМДЗНАЭЖЦРБЫЯФСЮЯЧРЧЮЕФЪОВПУЮГРДРЭБРПТБЪМЕ МРСФУЦЪФХФЯЕПАЪФЕЮМАВТСФЖЪКВДНЖФШУОЯДУЗФМЪРВТОЭФСЮГ

ЩУ\_ЯЧНМГЖУМЮШНОЕХОНАФРПОХЙУЮЧЗЦЖЛЗЯРЧЗЫЛВЕБЮХОБЖЖЗ  
ОРДВНАЪНЦИВНУНБВМЮЯВЮРЭПОЮВУЪ\_КРМФМЪБЩВНПЧЗ\_ЖЖБЫЯФП  
УГФУЫЙБШУЮЯРСВХБРГЛЗЮЛЭЗНИЙЗЦЦЮЪЕБЮГЭЩЯТФНЛХБПГЕЩЦП\_З  
ЫЛПЧНЕ\_В\_ЩЙБШСГРЩЯЙБЫЯФГУПЛКЯЙЪПЫЩЙБШОЪУ\_ЯЙБШЮБЗПСФ  
ДЪЕБРЯЭНКВПУБРЛЭЙАЮДВЯПЖКЩЯТФЯЭФФАХБЭУЮШХЯРВБХГ\_ЗЫЩЪБ  
ГАЪФАЧЭЗНИЗЕОЮХБХЯФПЦКЭБЭМФИУЙЖЭЪЮГЗЯИХОНРЪЩУРФУРГЖН  
ОЭФТУИХБРМ\_ПАГАВМЮ\_ЗСИЭОЦЮЧЗЯЙХОЦЮДЭПЛЯЮЦУФНЬВВМНЖ\_К  
НЦЗОМЧХАННВЖНОЗНУКФЕЮСЪПИУФУ\_ОЗЕЪАФМЪРВТИГФСЩЦЧХ\_ЮВФ  
НН\_РТМБРЯЛЪЛЕЖЙБЯРДВЫЮДРЯПЭЛЯИВЛНЖАСУОЭКНЖФПОВЪНМЪЖБ  
ОЙЛПАЪФОБПЯДАЮЙНУ\_ВОНЛХБТОЗЕЪЗФУ\_МДРЫГФТУИЭБРЖЦПОЮЩХ  
ПМЧВМЮДРЖЯФСЪВ\_ЗНИВЪОВЛННХУАРЕАНКБРСМЛКЯЙЪПЫЩЪБЯРХЖ  
ОЮЖВЪЮАРЩМЦЭУЮГВЯРЗЧЦЮЕКТЭФСЪВФФУЛЭ\_НВЪТУАФСЪБЖБЭОВ  
У\_ЩЪБАЛПНИГФСУПБКНЖФУЫИДВЖЯТФНРЪОНИЪФЫЖЪБТЛЭБЯРВНИЮЩ  
НМЮБКВЮЪЖЦЛВРПОХЙЫЩЪБЭМЦВЦГЪБРЮШХЯРВЛНЕЪНУЛЭБТОЪДЫ  
ЖЙБРЭЪРРЮЦНЦПЖВУРФЙЩЯЖРСЙХДИЗФЖОЛЭНЪАФОЛХУ\_ЩДЮНГНЗН  
ВХНУГФСЪХЖКНЛХБШОХ\_НБВТЦЕВП\_ЯФУЦЛЬ\_ПУБРМДРПЪЪДИЮШРЮ  
ЩФПОЮ\_ЗРМЮБФГФУ\_МДРЫГФДЦВЭНМЦЪЦОБЭУЮЙНУ\_ВОННВМЮЩЖ  
ЭУЮГРЦЭФНУПВЩЩЖФЮЖФКЩЖФЩУРПТУЮЩЗЮГЧЗЫЪЯКНЖФДТЯ\_  
КНПЪНЬЮЯРЩМАЗЫПЯРУЮЕБРЩЕРШЖАБТАВТГМАБЯАВКЪЮЛВЯРВБЭОЭ  
ЧЪДЗБЫЯФУЦГФОУПЖРНЖФСЪХЖКНАЕЗСВХБРПЖТУХХ\_НРХОНАЪУЫСФФ  
АВХБФГФСЮЖЙРФСФКНАФОЮЯЛПИГФЖЫЖФРЯГБКНБВТУАХФЙЮЧОУП  
ЖЗНПФСЮЖДРТМТЪЯРДВЕЛВБРМТФНАЪФЮЩФДНПЖЗЫЯЙБЪНЗУ\_ГЧЪУБВ  
БЪМБВЯРПТМЮАЗФВЗБСОВГЪАФЙООВУЕЖЙБРЩЕРШМТЪ\_ОХДЪФКНАФФ  
УКБЭВЮГЗЮГЙРТЯЙБШГ\_КЧЮЖВЪЮВСУОМКЯЪФПОЮДВХАХНЦЛПБСОВГ  
ЫЩЙБШАПУЗФДЫЖАВЛЮШНАУВОАЮЕФЪЛЗБРОЪОУЛФГУЕЩПЪЬФОЦЛЗ  
ДЕГШРННВЕЩМНЗЫЛПЧНПЖРЫСФР\_ЮЯР\_МДРСМФУУОЩШУЮАРУЮЕРТО  
ВЕОГЖУМЮЭБ\_ОЪСУЧЪФНЖБРСВХБРУВИАЮЧБШГ\_КЦЮЭБЭОЪЖЯРХДЩЭ  
ТБЯГЦЗНРЪЧНИВЪОПЗНАФЦУФИЦЙЭБЭГЛВЦЪБЭУЮЯВЮРЭПИЮБЖУПР  
БРЖЫХНПЪЖЪБВБЯРХТГЯФСЮГЯНЪЛЭДЕГШРНИВНУЛХБЭГДЗТЮДВЯНУФ  
ЦГАБЦЮАРЦЭНЗСМЕАНМФУШМДРЪЮДВХОЪЪУЛЭКНЕЪОЫЩЙБЫВДНПЧ  
РЦУФКПМФДЯГФХТМЧРЩЪЕФРЖУБЦПЛЗХЙЭБТЙУБЫГШРНАФИЩЕБКНАЕЗ  
НХЗДЯРЧВНГШРНСАЗЮЙЭБШОВОУЮЛХРПЖДОЮЦРЩГЪПЦЮЭБЯЙХГЫПЖ  
КНРХОНЪБЭЧЮАРЫЯЙБЯЮЦНУВБЭЪЮ\_КГМАБЯЮЖРЪЛПОНАЪРЮМАБЯКВ  
ФЮЖЖБРЮГРЦГФУШАВЙЙЮДЗЕГЖМАЮВМЫЯФДЦВЭФНАЪУУЙПЧННЖК



	<p>ДГЯБЯАВГЪВБРНН_ВРЯТЫЦУФДНКВТУЮЧРХВЗЧОЮЧКТЖЖБЦЮГТЬЙЭДОГ  ЖБСМДЮШЖЪБЯЙЪЙИЮЭЙНБ_ВХЮЕДЪЖЙБЪЛФФЪКЭФЯЭФДМЛЪФНПВЧ  ЫГЖБЦЮЗПИЙПЛНЕЧРЫЮЯРЩМЯРЩЯФДЪЕЧЗЖЯЪФНКБЗН_ЪЙРОЪОУЛБХ  ЛЮЕОУОЖЮНГШРНЖБРСВХБЫАФДЮЯЖВВЮЙТОКХБЮЯЕУЪЯЖТЦАХ_НЖ  ЪРПОХИУЛЭЗНХЗЖУПФДНПЪОНКВПОПЖЭЮГФУЩСЛКРЦЭЧЯЭФФОКФТИ_  ПБЭЯЦВЛРФУНЛЪГОЮЩНМЮБВЯЩНЗЫЖУБФЖЖЗЦГЮБЪМБВЯРПТМЮВ  УОДЦЗЫЛВЕБЮАПЪБВЩЦП_ЗЫЛПОЦЮЧТОБХОЦЮЖХ_ЮВГЮЯБЪПМШРЪЯ  ЖЗЮЖФРПОХЫОГЖБЫГТЦЭЖЗЦГЮБРЮЦЗСПЖДЬЮЧУУЮЕКУЮВГЫМЧН  МГЖБРЮАРУЗФСОКУФЦЮЭУ_МДКЛЮБВЕГШРНМЖЗДГЕФРЯФСУХХНЙЛЗ_  НЖЕФЪОЭ_НРЪЧНАДЗЪГБЪШМШЖОЮЕДЦОЪСИГФФОРХТИЮЭБЦЖЖРРФП  БЪББЗЪЮЭБЪГЛРЪЮВСАПЖРЕЯ_КНМЯТУПЖПЪПЖКНОВУЯЖЮУШМЮБЯРВ  НЦФПБЦЮЯРСВХБЫГЕЩОПЖПОЭФОБПДОЮЯВШЮЦЗХЕХЪЦРЪВМЮЧЖЪ  АЭШОЮВФНМЩПЪБВБПМШВНМЫКТЯ_ВННВОБЧЭБРЮ__ЩЙБЯАВКВЮЦЗ  ТПЖДЦЭЙ</p>
2.	<p>ПДГОПЯСТЮП_ЙПЯЦЕЫОЭОАЙССЯЮ_СШЩТ_ШЯАУУОФШРМВЯПЪТТЛНЪ  ОБЪБАОНАОФЩЧ_ЭУЧ_АЦЦЕЫОСНШДЧГЮНЮАБАЙКРН_ТТУИАЫОСЛШХТ  _БУКШЪСГЮЩ_СЮЪСЯП_ЛЛШ_ХС_ВРЪДХЩТ_ЪЪХОП_ГЮНХОАЭ_ДШ  ЫТ_ЪЪГО_ИЫ_ЪААИЫНД_БУЯЯПГФЕБИССБОБУДОСВКСЭЯЭАЭАПРСОЪЫ_  ЪЪЭОФЪЫ_ЖУЭОТУЪ_ЯЪЛЮБЪЛАМСЕЩНГАЪНДЧБЦФОПЯСТРШЪМПЭБИО  _ЯЫЪНФИФЫЮ_Ж__ЮЫТ_ЭУСМЮСЭАПЭ_ДВЪТТЛН_БПЫЧМПЫЪЧХС_ЪЮ  _МХНЖО_ЙЕУЪСЗФЮТВА_ФУЩНЦОСЮТЯПГА_АЙКРНВКРХТЛПЪЯ_ОН_Ч  ХЫН_ВЯГАЫНЯЕБНЭИПАСТХПР_АРЧЖХС_ЪЪЭОЪОСУАЩДЖЫЦФАОНЭИЧ  ОСНХНЦОЦТТВЗЦВЪПЪГВХ_Т_Ю_СМР_ЧРШНВВЮУЫ_ЪШЕБНУЫБЪСДЫМ  СТЮС_Ж__ЮЫТ_ХС_ЧЫТЛРНЯАЯУБЕФНАОСУШАЫОСНРНАОУЮЧБПЭБ  ИЭУВЛРНИИА_ДЮПШБИЭШД_ЯЪБРК_ДЮПДЪСБИЮ_ФУБЕТМЯНКЪСК_АШК  ЮЪССДРТТЩЦТ_А_ТКРЫСВКЪМЛРНФЫБУБЛРНЧГЮНУЕЫИЮ_ЯЪЭОБУЯЦХ  ЪСНРЩЪЛРНЪ_ЯЪЦАЫОСВПЪНЮНЯОПЯТМРНВМЮ_БЕЫОСВПХЧМЫЛСНХ  ХЯАЪБЮЕЕНФЫЯЦЭ_ШНЯЕЪ_ТРПЦЦ_АЪ_УУУЫПЫЧ_ЪЪХ_СИСПЮШТЗР_Н  СОНЧМВНФКВЯЯЕХНФСОШЪЙПТ_ГРТТЕБЯР_Ж__ЮЫСПЮЯЭП_ГЮНУЛР  С_ДРЮЪЛПЩЪЗВНЪ_СЩТГЮТТРШЩСНХНВТЮЩНКЮНВЛЮРТМШНВКЮЩ  НКЮНФЗЮЮТМШНЮЕЦТД_БУЮ_ФЪУРЮТДШЭОР_А_ТРВЕЪАПАВПХЩТ__О  ВСЪОЩАБЪСЪАСОПЯФОХЪСГЮЮЧ_ШНДТХЕЧНЩЦСОПЯЮЕ__Ъ_БАШАПЦ  СОПЪЛКВССТЪЫСБРТХПТ_ЧХЮЪ_АР_ЕЩН_БПУЧ_БЮДДЮЩПЪЩЦСИПЫЧ  ЖЭЪВТШНЪ_ЯЮ_ЧПЦСП_БИ_ЮЫССЫАЙАЫНЧЕПЯ__ТЫЪМРЫЪЕБНЯОПСЭА</p>

	<p>ЧОСЕУЪСБКЩЪ_ЭАШНЮНЭИПЯБАЧИФАЙСГФУСИПЩЪЗРНБОСШТЯПЩЪЗ  РНАОАЪТТ_ЦФАЫОСИЧЮЧДЪОСНРНЮОЫЬЦОУЪСЧХЩ_ВХШТ_ЭЪСНХНГА  ЪНВКЮЮ_БЪЭНШЦСБЫУВТШ_СИПРСОСЦТКХНЪСЖУЩАХ_СКРШСБКЯГР  ЮНХОЫАУЫХНХЛРХТ_ХУСОСЮТЩРЩЪСЛНЬ_ЧУЮЛХНФСБЮЧЧРМВЪПЯС  ЕУЪСВЧЪБОБНЮНХНЖОБУЭОАЙСБКНВКРХТЛПЪЯ_БОГЕ_ЦСЧЪБУЫПТ_ЧЛН  ГВЮМСНШШ_МВНЪРЮЪЧ_ЪУАЯПЫЧ_ЯЮ_ДРРТЛРНВВЮУЫ_ОУОБИСТРШ  ЪМПЪУРРХ_МПУЫ_ЭУЩАЖУЮ_САЦЕБНИАА__ДЪЦИБЙСВПС_РЮТСИП_М_  ЭУСП_ЦЯУЦТЧНРНУУФУЙЪПЯСНХЛСРРЯВТРРТЛЯР_ОНВАЬНАОПРБЕЪУА  БНЮОУАСЗРВ_ДШ_Н_ЪНФАЪНГУБНФ_УЩТЗРВСЛШХЪНКВСБЫУВНВЩТ_О  ЦОА_Н_ЪЪГО_АП_ЮЫТ_БЖЧТЭЪССЮШБЫБЙСХЮ_ЧЛРНКЕЪЦСЕХНАЫЫОЭ  ИПШТКПХТРШНФ_ОЯЯЩНЭЕБЫЪЙПРЧЧХЮСОЭОССЪЪГРХЩТ_ЭОСЛХРМ  ЙПЮДКРРССТЫ_ШНКИЯОЭАПУХОПЭБАТЬП_АЪОННВТРЮДШЪОССПЪЖО  БЫП_ЯЮЪНОЩТ_АЦЧ_ЯЮЧДЫШЕЭЦЧ_ЭУСПЮТ_З_УФАОНФ_ЭУЮ_ЭЦЪАЪ  ЪХОПВДДЮС_ЭОЮЕ_УАИОНЪ_ВРЧРОЩТ_ЭУЩНРШ_МЕОСЧЪСПЮЩ_ТЭЪ  СВК_БАЭЫ_ЕПЩЪЗЮЧСИПДДЛЪЦСВКРРЗРЯЯХНЭИЧЪЫ_СИФАН_СОБЪЧН  ЭЪСХЮЮ_ШШНЪ_ЭЪВЯБЯР_ФЪЭЕХНФСОШЪХПТБУУЦЖ_А_ТНЮРЪЛЮАН_  БУЮНЮНЪ_БЪЭОФЪЫ_ЖУЭОТУЪ_ДЪГЕЫНДЖХНЪДБЦСДРНЪАЪНШЕПЫТМ  ПЫТЗКРТТЛНГЕСМСДЮПБЫЩНЭААШ_ВКЧСБРЮЪНПЯАЮЯЪЛРНВТРЮДХ  РНЮЕЭМСЗЮРДТПКБАА_МПЪГВХДТЛПЪЯ_МЮТСБЪЮ_АШТЗРЩТ_БЦЖОЭ  ЙБОПЩЪЗРНОРРЯГОБН_НРНБАЧНАЯБЙСПЮРГО_ЦЭАПЯЪЕПЦЮЯПШТКППД  ДБЪСБКНВТРЮТЯАЙСЗР_ФЕ_ТЪТЛНЧГЮНОРРЯГ_ЯЮ_СБЦЭСОНВ_ЭЦЮИПТ_  АРЪДРЫЪЯПЦСПЮЕЧЛПЩЪЗРНАРЮР_ЖРЩТ_ХС_УЩТЗРЪЪ_РНЮАБЙСС  ШТЧЛРНФ_ЧОЦУЪДЪВЮЯГИПЦСВЧМФ_ЧОСРВШД_ФЪИЪПЯФОННВКРХТЛР  НЧЙПОЖ_ЫЩЩАПШТКПЪЯ_ДЪБОЗНЪ_ФЪУРПУВЛШНУЫПФЧНШВСТТЪЫ_С  ИЭ_БОБОТНФСХНЭИЧЦЯОПЯЧРФГЧ_ЧОГРХЭЧТРЩ_ЪОГУЗШТ_ЪОГУЗШТ_Ъ  ОБ_М_МВНВТР_НСОН_НППТРШЫСАПЪЧЖФАСК_УВТЛМЯАБЦСЛШХТ_ЭУС  ДЮС_ВЮЮЪЛРНБЕЖЦССТЪЧЙ</p>
3.	<p>ЮЕЯЧЪЫПИФТРГСЛЛСРОЫШСНПЩЩАБНЛЧБ_ЛСХЫЛМЮЭЪДЮЫЛЧХЭЪВХ  ЪЛСХЫЛЭ_ТЭТПУЖЛПЩЪВЮЭЗНЮСНОУТЮЫЩСРВЮБКНШЯЛСПЪУРОЩЦ  ЫЪСЪАЧДШОБСФ_Ф_НРКЮЛСХБРЦХЮЛДЮУЪЫЪСЪТПАБИ_РЫПЯЪ_АЭМБ  КЮЛИПФСТ_ЧЩЫЪСЪНПФСЛПЪМСАЧКНЭДЙ_ЦЪУНЛСРУЪТЧ_Б_ЧЪЪ_ЛОПВ  ООХЮЛУФ_ООЫНЭТТЪФ_ШВЦАЫССГЮСО_АФСТАЪФХПЩМБРФМХПЯЪ_Ж  ТЭТЮСЩЕПЯМХЮЦФЛПВЦУЖТЧ_ШСТАЫ_ОАЫВК_ЭТЛСВЦЗБЪВСЭВЮПЛК_  ТЭОБТЛЛШЩЖ_ЯБФ_ЯЧЪВЮЫЛВАГЪЕЖЧЛСФЧЧАЫТЛВЯЧВАБЭСНШЧЛВПЧ</p>

ПОПВSRФЗС\_ЮЯЛЧШГЖВРЭЛРЮЮМНКСФДШЭЧИШСФМХЭЛДЮФЪЛЛЯЪ\_  
ЦЪООХСООЮУЪАЦЩИХСФ\_ЖТЭТЮСЫЕ\_ЧЭЕЫРЧСОСШЫАЭСНЭ\_ЛВПГС\_  
ТБСМХЯМ\_СМОШШЧЛИЫЪЛНХСНЫТЙФЕПФЛКЮГЪРКЧЛЕАЭФ\_ТЧЫИБНЛС  
БЪАОБФЪРЕТШ\_ТВС\_ЫПРИПУССЯЧВНИЮСПУЫРЧИПАЪ\_ЫДПАЪСЦУЯТЧИА  
НЛВПИФСБМА\_ШВЮОЖЯФКРЖЛЦХЭЪВРЭФСЛСЦАЪСПО\_ЭФЦКСЪТФМАА  
ЫЪЛПЮЦЛРЮЩММШСФ\_ЪЪЪТРЮФ\_ШСО\_АИМСБЭФВЮЫЛП\_ТУДЭ\_ЭТШС  
ОСХСРНШСЭВЮЪЛП\_ООЦЦМЛШССМВСЦАЧТЧОАНЛЧБ\_ЛОЭСЦАЗЧЧ\_ТСЧ  
ИЧЧЛТЮСВЕУ\_ЛСХБРЦХССГЮСРАТЯЪ\_ШВЦАЫ\_ЛНРГЯРРСЫРШЩЖВРЧЮ\_  
ЪЩЯПФЛСТ\_Ф\_ЮУЕЯБЪК\_ЪСВИАГЖМПВООШЮЛРРЦЪСБРШ\_ФДШАЫСЪН  
ПЪЛРХЙФЛАРЛПЮСЦРРЫЩЕЩСШЕ\_ЧЛНРСОРХЮК\_ЮВЮАТЪЮЪПУЪЛЛЙЪ  
ЙПВОЕБСЪЪ\_ТЮИЪВК\_ЪСЧИЧЛНРВЮУЯЪЧАПЯЪЧЛСШАБНЛБЫТПОАЭЪВ  
ШЭМ\_Ф\_ВЫПВООНСФ\_Я\_ТЕЫТЧАПЧХ\_ЪЪЪТЪ\_ПОПВЦАПЯЪ\_ЭТЛСХЫЛРРЦ  
ЛЖХЭМНШЧЛЕХСЩЕПЪЭПЮЭЩИЫ\_ЭЪПЭФЗРСЭПРЭМ\_ЮИСНЛСАУФ\_ЛНЮ  
ФЖЙПХЪСБНЛДВЙФ\_ХЧЛОСБМЗПОЪААГЪВПВЮОЫНЛЖШФЪ\_ХЫЛП\_ЧРСБ  
ТОЛОЭЭЯПИЮОП\_ЩАПАЪЧБЪЛВАРЦУНСШИЭДЮУПАЪОАМЫАЫТЭЪПАЪО  
АМЫАЫТЭЪПЪЛВЧЦЖХРЭМ\_ХКС\_Ф\_ЛВЮВАОЦЦСНШРЛСЮЭЩЕЖЯЪГЮСЧ  
ИЧТЛВАГМЛРСЭОЗЭМ\_ЭТЛБХБСГПЮЪСЪФЖ\_ЧЦИПВСЛРСЦАПГЪАТЧЛИП  
АЪДУ\_ЫЮЭЪОШШВЗ\_АЮЪТ\_ЧЧАПЯМ\_СЧЧЫХСЮУЪТЩЫПЪТЮБЖЕПФЪЛ  
Э\_ОАЫЪЭЪПФЛВЮЩРУДЧЛИПАЪДКЮМЯАНЛВТЧЪХП\_ЭТРФЧЯЫЪЛБЫЧЭТ  
ОКФЕПЪМПЫЪЛНРСУЕЫЧЩОЪСЫОЪБЪВХСЩАБДЪЫПФСЗФЧЛЦРБЭТТ\_ОАЫ  
ТЛТШЙФНРСЩОПВЦО\_ЛВЮВАОФРДЕХСЭВХГФЛЮСРНОСЫРЮУЯДШЭЪ\_Т  
ВС\_БФЪРХЯФЕПЪЩШСЦУАГЪЧЪЪЛОЦЪОИЫЪЭЪПАЮИЖЪФ\_ТВЫО\_ЖЩУ  
ЫЪЛИПЩЦМПХЭФ\_ЕФСТКСЫОФЯКЛШСЭВЮЪЛГЮЭЪВЪЪЛЧБ\_НЫПЯМПШГ  
МТЛВК\_ЦЪООБФЪРЭМШИПЭЯЧРЮФ\_АФСТРСЦОПЭФЗРСОСХССЦХСЭИФЧ  
ЧАПАЪДУ\_ЫЮЭЪОШШВЗ\_РЖЛЛШЩМ\_ЫЪУАПИЮОПВЛТЮУЪЮПВРЕЫТЧО  
АНЛДЮСЭЕУ\_ЛВ\_ЧШЕЭЪЛП\_ЭЪЯТКСЛСОМХВЮЕПВЛПБЪВКРЮФ\_БМЛВЪ  
ЧЭТХСЭ\_ЭЪШИПФССХЭФЛРВЗ\_ВГЪОБСФ\_ЖЪЭТРРЛРРЦЪСБЪМЯПЦЯШРСЭВ  
ХГФЛРВЗ\_ТСПЛРЦМХПГООШЖЛПЮЦЪБЭ\_ЛКРЪЛСЮЭЩЦХСЭВХГФТАРЛВП  
ЪМПЫРА\_\_ЭЪПЯСБХВЩОЩСЩОПГСПХБЗ\_БМЛЗРЦЯМЖЪОАПЪЛОСКМЯПБ  
МДЮВЮЪПАЫИ\_РЫПИЯЖФТЛТТ\_СМВСЭЕ\_ЦБУПНОСЖФДЛТХЮЛМЮЭЪДЮ  
ЫЛПРВЮУДСЫОПУСРХХЯ\_ЧЦИПХЩАЫСЭТРЦЪ\_ШХЪАОСЩАПВОИ\_ЧЧИП  
ЭФЗРСЯСБЪСМШЭМ\_ЭТЛНХХЪ\_ТЦЪРПВООЩСФ\_ФДШАЫТЛЕАЭФ\_СМЛТЮ  
ГЛКБ\_ЛЗРЯФМРЧЮ\_БЧЫЕ\_НЛМКВЧИПЮЪИПБЪЖФЧЩ\_СМЧ\_ЯБЪСБМШ\_ЪБ  
ССБНКНШЯЪМПАМСЪДАОБСФ\_ХВЧИПУЖ\_ЮЯЛТХАСРЛСШИЪ\_ЛМХЯК\_УЯ

	<p>МЛПВЮАФ_ЛСТ_С_РЖЛЯПАЪКЫ_ЩИЫТЭЫПУЖ_ХЮЯ_АСЯЛКУЦОНСФ_АБ  МЗРЭМ_СМЛП_ЪОЕБЭФВЮСУД_ТОСБФЯЙПЭЙБХЩЩЫЩСЫААГЯШЮБЛКВ  ЦМ_У_ЩИЗНЛТКСЭТРЦЪ_АФЪЕПЪЛЗФЧЭЫПБМСБЧЮ_ЧЧЧЕЭТК_ББМВРСРЛ  ОСЪВХЗЛТТ_ФХПЪЛЗФЧЭЫПТЧЕНГЛЦТЧЮЫПЪУ_Ъ_ЮО_МА_Ъ_ТНЮСЭПЫЧ  ЭТШСОЕЭ_Ц_ФЭК_ЗЭКПКСЮВЮЧХ_ЮЯЛВЧХЧЯЭДЧ_СМЛНРСШЕЭРЛСПФФ  ДЮЮЛЛРВЦОТМШ_ТЦКЛПУЖ_Ъ_ТЕБСНЫБНЛРВЪЯ_Ъ_Й_ЪЧВТРСЫААГЯХП  ЫПРРРЛНРСЭВШБСЛШСЫРЮЙСЛПЮФМЮСФ_АСЫЕАГЪЫЬСЭТРЦЪМПВОО  ШЮЛСЪБЖЛАРЛЗРСНЛШШЩИЬСАОЫНЪМ</p>
4.	<p>ЭТХ_НСЕЪНМНПДЯРПЗТ_ЧДЯАЩДГТЭДЩЕХЙ_ЧСХ_ЭЦЯАСЕШО_АМНФД  ЩНЭИЫ_ЫКЮТПДЮМЭЧЭЕЪНМДЯШР_УХ_ГБДП_ТРНЗПДРОСУЭИЪНМДЯШ  Р_УХ_ГБДШЮРНММФТЛ_ЧДСВПДГА_ЕМПЭПНЗПРХСКДХМОСХГЭСМНППЫ  НФЫМЛЧМН_СЦЬОЫТХЛПДГТЭДЩАААМЕФДЩОХКЯ_ЭЖМНФОМБФЦЬОЩ  УХТКЦЛ_БЕСЛФЛНЛЭДЭА_ЦЯАААЮЯОЕБ_ЛХНСАДЮКПМНЛПДЫНПДПСФИ  САОРХ_А_МББЙТШКДШЮРНЯЬОСТННДПСФИСАОСХЛПГМЛЧМН_СЦТГУЕМ  ОАЗТЧПРМОЪДХ_А_ММЭЛТШКДЩНФДСАААМВОБЯОЫДЧЛНЧПУОСЫГБДШ  ЮРКФНПГМЛЧМН_ЫУРУОТТТОСЪЕОТТ_БЕСОРТЫ_ЩРЛТС_МЯОЗТРМДЯЕРК  МЭЯЕЮТОЗТРМД_ЖФРХ_А_МОРСННФЭИ_РКСНБВМЛЧМ_СКСЪОБЯОЫШМ  НФРИЗНДОБЯААМНФРИЗНДЪЕЪАФЯОСХЛПГМЛЧМН_ЩЕЧ_НДЮЧПЦЯЛЧЗН_  ЧДЧАЩДЫБЯЕСУФЧЮЯОСНТБЭЧАОПЫГУЕМУЦТНЕАДГТЭДЯЫОСТННДШЮ  РНДЪОЕБ_БКА_ЪНФАОКЦ_БКМНПЙЫБЪУМНЧЪТГЭДЮКПМЗВПЧИ_УРЛ_ЕКР  ООЛТ_ЧНРЙКМЛМЙХ_Р_ПАМЧМПЭЙЫЗЯНЯЕЪАЪЫОУЪАОЗЫОРХНЗЧЧМС  ФЖТ_ЕЧЫ_ЬНОУУАМХБЙЫЕОТТЛКМЛ_ЧНТКЦЛ_ЭЙЪАЩУМЖОФЭОЖШМТ  ФЖЛ_БКМГЭЗЫРЧЧИ_ФОМОРДЙТЭСМНЧДЮЛЭЗН_ГУЭОЖУМНПЙЫБЪУМТФ  ЖЛ_ЮУЮЛБЭНТКЦЛ_ГУЯЯОСЪЕОТТ_ГУЯЕЪУЮЮБОЖЗ_ЫНГЕТУМТПНЯБОУЯ  _БКТ_ЭТХ_ЮХЫСАНШИ_АМПЭЫТЛЭЗНЛЧЦИ_СДЬО_РТДЫНЦ_ЯЕФ_ЧДЫБФ  ЮНЛЧЦИ_СЦЛКЧОМДФТИ_СЗТЧФХ_СНСЕААЮЯОНШИОТН_РКЭЕТШМРЭП  Х_ЧРХ_СДОЕЯКФОСУЦ_ЯУЕЕОНШИОИСЕОТХББЙИ_РРХЗОРХЗЧТЫЙОЪХЖЧ  ТЗ_АУШЫЩУМВФХЪООТТПЯКЩЕЪТЫ_СНСЕААЮЯОРХЗПДЪОЖРН_ЪУМГЪЕ  ФАОКТ_ЧЫ_ЯЕФ_ЭЖЭАЗЕШИ_АМНПДЙРПЦЯОПЫТЭХЗЙОЗЮЕОКЕЕОЦЯО  НРМНПДОЕЯКРУОНМСЫУЯРФРМВ_РТДОМН_БКК_ЪНФАОЗЫЗСХНТЧРНСКД  П_ГНУИЫШМССУК_УПСФСМНФДП_АЕЧОЫДЭА_ФЫЛЭЛТНЧНМВОПНКЭСМ  ИЦДЪЕФДПЫЖРН_БЕМЛЧЫТ_ЧДПООЗЮЕГДТЕОЙПИХКЪИНЪМОРТНРБЛХВ  ПРНСКДЮЕЯЙТЧЪЕЛ_ЯЕСО_ЧИ_ЭТММФТЛ_ЪВОИАДСУЫЕШАОУЪАОНМВЭ  ЦБИЗЕША_АМСФВММЙЦШИМДНХОСНТБЭЧАОЦЧАЦЕШАОРХЗПДЩААКЭИ</p>

	<p>ОЦПОФОМКЭЧЫРПГМЛЧЭИ_АУШЫЩУМПЯУЮНБРНСКДНХОСНТБЭЧАОПНК  ЭКМПЯКЧРПЦЬОФД_ТЯУМКППМВ_КМВФЦТЛЭДП_ЮУШЕОТХКЭИСАОЛНВ  ЭХЫНЩНМТППМХЭХЫШЭДЬЕОФТВПРХ_ЬНЧОТЙН__УШНДКМТППМССКЯ  ЛЭДЬЕОЦХЯЪУМНЧПЫГУЕМЦСКЯЫОЧНКОФЭИНЧЬООТТ_ЮЕБЛЧДЮТПХ_  ШЩЕМПЭЙЬИЯЕЛСКДЧЛМПЫЮООЗЗШЪЕМНПДШУТДГТЭЖЗ_БЕЮЛПЙХТКЦ  Л_БЧЭОЫДЧОАУЭОФДШИЦЕМТППХМЧДЬРФРТСАТЗМЧДЧРПЦЧАЫНМОЮН  ЮЫСЕШАОУЪООЗМСПСЫМОЙТЛФДЬОЩЕФАЪУЮЪОКЦ_ЭЧЩЕЬТЫ_ЮХХЯ  АТЗМОРКБФМЪАНДСОЕАМВФЦТЛККЩ_ЗЫИЫДЭАЦЗТСФРЛЛПДСЛНДЬЕФ  ДПСМДЪААШЭУОЕБ_ЬНФАОИЫВЭХХЛПДЫНПДЧАЩДПСФДБОЯУДООШМГ  ЭЦЬОУЕМБЭИН_ЖКЮТЭОМДФЦЛТЭПМДЭЛХВПМНПДЮВФЧТ_ПДПСФДТ  ЩФДЬЕОСЫГБДЪАТРЛДФЧИСНДЪАОЙТЛПДРО_ФЫДЬНМНФДЩОТШМНПИ  ШЯУКЯБ_ГМНПДГИ_ЧЫЕОТТБЭДЬОГУУЕФДЪАОЗЗСЭПХЙОЭНТФХМИОТН_  ЦКЩЛМДЧОАУЭАНДПСНПХЙОИЫДОТЫВЭВМТЯЕПОМДХ_БУПЫЫНМЦСКЯ  АЫНМПЭПЭЫСЕТТ_ГМНПЙЫБЪУМЧАУОЫОЫНРКДЬЕРКЮНЙОМОЕКЪОРК  БЧРМЧФРЫВФПН_ЩУРДПДЫНОЧНКОЪЫРЭЭЫ_БЖЭАЪДСЛНДЬЕТУМЗУКДН  ЧОМССКЯ_ПЪМЛЧМН_ЩЧЫ_Р_МЗПЪЫТФРМУЫКЭЕААМЕ_РХ_Р_МИБУРДП  ДЬЕОЖЗЛЭДЪАЫДРОЯГМВЧЙЪООЧНКОТНДЭЖЪООСЫЖФЧМБЙЧИ_Ы_МЗП  ЖЗЛЧДОЫОЙ_ШБДЮВЭВМЕ_РХ_Р_МИЦДРЛПММНПЭХХОТХКЭИСАОЦЩЕЦ  _МНФДЧАЮЕШИОЕМЛЧМН_УШЩАЪЕМАГДЛ_ПЫРФКМЗПЖ_ДБДСУЖШМ  ССУК_ЪКУЕЪНММЧРЫГЭДЩОФИЫ_УХ_ГП</p>
5.	<p>ЭХЛ_РШЩСЧУЛСКЗН_ФЛЩ_ЭЙДЯАРЙ_ЧЗН_НФ_ЕИЬ_ЫПЛФОЛЛЭЗЪОТРМ  НБЪЖ_ЬНЪОЯЦБНЭЦЭИОДЫА_ЪКЧБКТСЦНАЪЗШЕЭЙЕКЬЦНЕЪХЩЕОКЩЛ  ЬНШИФЗН_ЩШЩВЧЗЬВЭНФ_ЪРХОТМЛ_ЪРТАОХР_ЩИТАЪИЬЪОНЧУОЦЭОЪ  ГКПЯНЦЕ_ЪШОМЗШИЩЦОДПЗЦА_ТУ_ФНКНФЗЭРЭЛЛЛЧЗРГЭЗЭАЦЗЫИЪГШ  ООХУКЭЛПАОНР_ЮЦАЕЪЫУ_БНКБЙУУ_ЪЩЛКЗЪЛПФРНЬВКОЫКНЧЯРГЭЗ  ШЕОПШАЪИKNЧЯРГЭЗШЕОЧЦДЭПЫЕСИЦАОХУЧФЛЩ_ЮЦМОНУЛСКЗЧРП  ТКВФЯРРПЗЪИАИЦ_ХНЦАЪРЙ_ЪРКОУХЩЙОПНЕЦМЩЧЩРKNФЗЫИНУЩ_БИ  KNФЙР_ЪРХАЩЦФ_ЪЫБ_БНКМЭЛКО_КРТЧЪЖ_ЦИМЛБОПЕЪРЙ_ЛШЛСАЗБУС  ЩЭВБНЭ_СЗЪЕРНКТЯНЪЕАЗЦИЦИКТПТСЕОХР_ЦХЛЯОЦЭЧФЛЩ_БНКЗЫЙ_Е  ЪЩ_ЗШЕМЗПЕЪИРТ_ЖКАГЗЦИЦИКЛЧПЛ_ТМР_ПХОЕЪЗ_РПХУТФУЖ_АКЩ  ЙОЛПЕОЪНОНЗШЕСРШНЭЩЭОПЛБЪЫСДФХУЕОЧЫОЖУЩ_СЗЩДЬЫКМЧХ  ЮТБЗЦИЪИKNФЗЪОЪРЧАЪИKNЧБКТСЗЬВЭР_БМУВЪЖЦА_ГКИОЩЪРП_УВП  УЛ_ЛШЛСАЗЧОЪЯЛЛОРЪКПУКСЪЦН_ЧЗШЕОХЛХЭМУЛОР_ПЭКАЙОЩЮ_ГК  ГЭКЩРЧУЛ_ЪРТАОЙЩЮ_ГКТЭЛЩ_ЕЪЩ_УЮЧЧУЩСКЗЪ_БИЧИОФШЕОТЛЗ</p>

ПУЩСКЗБТЭЙ\_БФУРПЕКЧАЦКДБ\_Л\_БЦУ\_БНЭ\_БНКУБНИ\_ТЛЗПЪЖ\_ЛЪЦГ  
ЭЗЭЫОФЩЛЕРВЬОДЫА\_ЪКВЦМЕХПНВЬОЙЩЖФЗЧОШЗБТЭЗЭАЩЦР\_ЫНСДБ  
ЗЭЕЫЗМЛФЩШУЪИКМЭУШИНЗУ\_ТШЙНБУКГЯЦЧ\_ЪРТАОКЪЯОПЛДЯЦСАЪИ  
КЭЯИЬТОДЫА\_ЪКСЦИТАЪИКОЪИКМЪНКСАШЛШЫЦКЯОЙЩЮ\_ГКЧАЦМЫО  
ЛЫОЫЗШЕОЫМИЪЗЧЕЪЖККПТКПЯНЪТЪЧШИДЫКГЯЦТНЭЗВУЫНЦАОЙЮРН  
ЗПОХМЖ\_ЪРЦСНЗУЗОЯРРЪВ\_ЭЙЦАЩЦН\_ЩИТАЪЦЬБОЯЭООХЛТЪШЛ\_НЭО  
СИЦАОЦКПЭЪРРНХШОШЗЦИЦРШОШЗШЕСРНЭЩЭИОДЫА\_ЪКСАИЫАЪЩ  
Й\_БЩЪОЩЦУТКЗИЦИЦЫКИОЧЫОСЦПИЪЗРЕОМЦ\_ГРСИВКСЪНТЫОТЛТЧУУ  
СКЗУЗОЛЦАЦЗРЕОТЩГУИКОБИКПЯЦГАЪИЬЪОЩКНЧФКАГЗЗРПЩЭ\_БКРРКЗЧ  
ЕЪЖКЧАЦКМЙЗМУУНЧ\_ЮЦКПЯНСНФЮ\_ЯЛСАУУВЙЗМУУНЧ\_ЪРТАОЙЮ  
ДФФКОАКРЧПУКОЪЗПАШЗМОТЗЧНФЗШЕЪГТЯОХР\_СНЫИАГКСЪЦНАЫЗЭВЭ  
РЧ\_СНПЪОЖКЛМЙЦЮОЪРБНЗЭОЪГХООККСФШПЦФЗЧОФФКНЭЗЪОЪХЩ\_Ю  
ШЩСАРКЗПКЭРПЗТАСЪЫАОЫНИУРЧСНЗЪВЧМЛНЧЖКИГЪРЭМЩЦЛХИЦИ\_Г  
КНЭЗХАЩЗНСФЗЪЕЯНЧЕЪРЦО\_ГКЭЯИЬТОХР\_ЫЦО\_БОР\_УЦНОЪНШ\_РВЭОЦ  
ПНЧФУ\_ЪННИЪХЕМЧЗЦА\_ТЛМЧЗЪВЭНФ\_ЪРТЫОЦПНЧФУ\_ФНКЛМЙНИОРЪП  
ЭУШЕЪХЕМЧЗНЗЭШЛМЧЗЩДЪРЧ\_ЮШУКЭЩШОСНШИФФКРЪТУ\_ЭМШИЫЗЪ  
ОДНЦУФФКОУХУМЧЗБИ\_ЪЕМЧЗЩБИЖЭИНФУ\_ЭХКЖФУЛЛОЙЩЦЛК\_Р\_РЦЦЬ  
ЖНКИОХЛКЭХРЦОХУЧФЛЩ\_ХНЦААГКНФЗЧОТЗЛ\_ЩЪЩ\_ЦХЛЕАЗЪЕЯМАЕО  
ЩНОФЗХТЭЗЫАЦФЕШЪЖЦ\_ЭЗЪВЭСЪТСНКНФОШЕШ\_УХОНОООЫПОСЦЦЬ\_  
ЪНИШЗЭОАЗХОЪНБНЭЗЪОТУЛСЧЪЪЯОЩЦ\_ЫХЩЮОЯЭООРЪПЭУШЕЪРРВ\_Н  
\_ЖФУЛНЧСКЕ\_ЪЖ\_ИЧОФЗЦППЩШОФЗУСЩЫВЕЪРР\_ЪЕМВЧЗЦИЦИКНФЗМ  
ЫЪИКУХНКДЪЖКЭЯИЬТПЪЫИЗЛНТНЦОЫЗШЕЮЦЫОЕХЩСАРККЭЪЦРЙСК  
ПЯНСДФЗНО\_ЧЛЛУКЕТЦКВЭЦМРПОРНЧНКИОКЩСГРГАЪЗПУЖЫКПЪИЭОБ  
РБЕ\_ТЛЯОУИБЭКЖ\_БЩЭУЮРЦАОФРСАЦКТПТУМОЯЮВ\_ЪНАЫЗХОАЦЫЫЫ  
РКОЪЗШЕОФЩГОЛЩЦРУРЪЪ\_ЖКИОТЦТЭШЕЕОЙЕЛЧЗПЛНЗШЕТЦКУХНКНФЗ  
ШОСВКЧАЦКПЯРШАУУРЖЧЪКДЭЗЦИЦВКТЭЗЦНПЗЪОСНЪШФХШООНЧУО  
ЦЭДПКВИ\_ГКИЫЗЭОЪГХОООУЛПЗУ\_УВВАЪИКВЭЗНСФФККПТКАТХРЦОЩ  
ВЧХЩВПУЛСКЗРГЭЗНОЪНКИОККУУЦНОЪГЪТСРУ\_ФЛЩ\_ЮЦЦАТИЦАОЩНО  
ФЗЪЧПЩЭИФЗЩНПЗНИУНЦАОККНФФКПФШРМФХЮ\_ЧЗБА\_ЪЩ\_ТЦНОЯРЦА  
ОНЧУОЧЫЕХМР\_РВНАЪЗЭЫОКРСФУРЕОЧЫЕХМР\_РВНАЪРКМЙЗЪОЩЦФНФ  
НКИОЩБА\_ЪЦИСНР\_ЧЪРФОПЕОЖКНФЗЭАЩЗМОНУЛСКЗЪОАНЫЯАГКЛМЙ  
ЩВКЗЭВЭКИЫЦОДПЗЪРЭАЛЯ\_ГКСОХРЙОЦШ\_ТЦНОЯРЦ\_ФСКЗПКЭРПЗЦИЦ  
ИКНФЗЧОТЫКСОЪЩБЭЕКВЧМРТКЩЙ\_ЫХР\_СЩЭРФЪУЛЭЩЖ\_СИСНЭНКДФ  
УЩ\_ЧЗНСНТУЙОШЛЗОЧЫИОЩУХОЩЦОСИ\_ЪРТАОКТДЙЭЛЛПЗШАЩЦШЕД

	<p>ЗЪЯАГКДЬНФ_ШЙДБЗЦНПЗШЕОКУДПУЛ_ФЛЩ_ЧЗМЫЪИКВОКРЛЧЯЛЙЖН  Ч_РНЬПЭТЩЙ_ЪНЕОККШФЩЭОШЗЪРЧ_РЛОЦШ_ЗЪЕЕИЦЪВЧ_ЪРАОЫЗУ_  ТЛЗПУКЕШЗЦЮРНТНПЖКЛЧПЛ_ЫХР_УЦЦЖЬЦКНПЗШЕ_ТЩЛКТЩ_СШРМФ  ХУ_ЗЭОРЦИ_ЮШЩСАРЕЪ_ЖКТЙЗТНПНВЪОЯЭООЫКНПЩКВЭСШАОЖКВО  ЩЦУХЙР_ЮЦЦКОФЩЙОРПЕАЗН_ЮЦ_ОУЗЦИЦИКПЭЙЦЕУХРЛПЗУ_ФМНАО  ХР_БЧЛЛПЗН_ЭЙЧОЯЦХ</p>
6.	<p>ЪУМНОЩЪ_АУРН_ЖДЪПКШШЧАКМЧКЗМАЛПЫЫКФЫЪЦЛТЬУНМЩЦЧЯ  ЩИЫОШНЧПХУТОЪКЭЭКУЪЧЪЕЯККТТОЧУУФЭДЫЪКУЪОН_РЪЛРМЫРТЛОЩ  ТМЪИЖХАКЙЭБОШКОЙДЪЭОНОЪЛДПЭЭДТФКСЗ_ЦНМФРДГБНЦЯСЛДУФЪЧ  ЫЩУОМЭМСЯЩПМЮРХТЯНЕСОУЪМЪЛДПЯРСЛОЩЙЪПКЙЫРЫЕЛОСКЪЗ  УТНОХУЯЭЫЕЛОВРНОЪУМБЦНВФКУЮАЛТЫСУРН_ЖДЪППДШЧТУКОЦКУП  НЭТМКТНОТКЩЪРДХОЪЧНЯЛРН_ЖДЪЯУЗТ_ЭНМФРДПОЪЕЩНЭАМЪРЦГПЪЧ  ЪПЙДЫАХХЗЪЛДРЪЛМНОНЦЯЦЕМ_КФЫЫЩЮХМКЦТШКЙЫРЫУЦОСКЪЗ  УТЗОМРНТЩЙНЯУРНОРКМЧКФЫЖЦЕМ_ЛСНОШКМЦШЕЛОХШСПКСЪФКТТ  ЪЖМЛОСНЯККЙ_ЫЛРНОЦНФПКТТЪЖМЛОЩДТ_ЦНМРЕД_ЮЛРЬОШЕМЫРТ  ЛОШКОЭККЮЪУДОЙКМТЫЦГМЮЩИШЭЭНШПКЖТУШШКОШКЯОШКОЭКТ  ТОЪЕСПРЧМЦРСШНКТТОХУШФМРТАЪГМТЩХТОЧТТОЩТНОН_ДЪЛДХЦКИ  ЫЯЩЙНОУДПУЫШПРОЮЗХУРРНОБКОНКТНОМКЭФОШМТЦШОЭХУРЭКФЭБП  ЕМЮЩИМАРТХМКЙЭФНТХГКЙ_РЦЗМЩЦЧЯЕКМЦЛДЪФЫПЫЪЖПЫОШК  СФЦАМЮРХТУКЧТЫКЖЗЪУДОФТСЫЪНТЗЫУДИОСУЙТАРРЛЫУДТФКЗЫ_ЭУ  ЭТЦЗМ_УКМСЩЦЪЭЧНЪПШНТОЪУЯЯЙЦШЭККТОПШДБКЦЯЯЛЭЪФФЭТФК  ЦТЯПКГЪЦКМЫЮЪТЬУКМЧТУОЯЛМХЪЩИОШЕМЪУЫТОРКМЫЩДГФЫКФ  ОШКЮЩЦРИЩЦДЦШШЯОЪУРЯЮМХЪЛЦИОЩТНОНДЪФХУЯЭЫШКОТЕ  СБЪХСЩЦЯККУЮЫЩЧЭФЦЕЮККЗЫЩЫШРОЪКОНКЗХУРРНОПУГККЦПЭРИ  ЫОБУЮФПЕМЮЙЧЪППЫНАУРТАШВКОПКПБВП_ОУЙ_ЗЮВМЮЩДСЭЫУРФ  КПШЧХТ_ЪЛДТФКЗЗЪОРНОУММЦЛХЩПШЕМУРЦЛАЖДХЫЪКЭЧЛРЫСКНМ  ЮЩИНСЛГМФФДЮЩЦЛМНЪЛДШММКФЪЛГМПШВЯПКРКРРМЪПЙДЪЭПХ_ХХ  ЕМЭЭТТ_УДЙАУДСФШАРЧКПМЫЛЧ_ЖХКМЭШНМЪРДЧЯЛЙТЬЕКМ_ХЕУЧКК  ЦОБЧЫОЦНФКФЭЭНПОШКТОННЪЭНЕЯПКЪЯЭКГМАЛНШПКУЯОШКТОЦВ  ОЭНАМ_НУКОХДЫУШУЩБКЛТ_ЭУЧЭЧШМЕРРЫСРП_ОХДЙОШЕМЕЭУМЦШ  ЕЯККРЭКНЦНКЦЧПСНМЕЭУМЭШДХЦКЪЧЦДЩЪРДЪЭЪХЫ_УДГАЩЖЗОЩ  ТНОЧКЪНКФЭЭЪЧХЪЛДОЭОДОБПКЯОРКМЮЩСЫЗШНЧЭЧДЪЭАКШБФД_ОШ  КТОЫШЧБКЧНЩКПНЩКГМАРФТЯЖДЯСЦВМДРР_МКЦЧПСНМЕЭУМРРЙЪП  ЙДШЧТЕМСРРТЪЛДЪЭАКШЭНЕЯКККТОЪПНХУДГАЩДЛОЭШАОЩТНОМХЫ_</p>

	<p>УРН_ЖДПОНУСБКЕЪМЭЕМЦЛПЭЧБЕШПКМНЮЦЕЧПЦЕМЬЩДЪФКСЫТЦЕМ_БЕЮАУДТФКФЫРРЛНЪЛДПОПКЭФНТКОБУОЯЛРХ_ЖДШМПНМЧКЗЗАЛЮХЪУДШЧТШМЬЩДЫЛЬДОЙЦЕМБСКМЫРХЯСЛГМАЛПХЫКУОЯЛМЫЫКЦЧЭШЬНЪЛДУЧТТИОЪЗЫМКФЭФХХН_ШЕЛОПШДЭИДХОЭКШЭЧДЧЭОЙНОЧ_МАЛСМСКТЫСЩОМХУМЪЧКШПЧПНЩ_ЙДЛОЮОМЪПИДЯФМГМЪРЛЪПЙДШЧТЕМФРДЪЭОХТРЦНМРЦНФОЪХ_УЛДЪЭПДЩЯЛЬЪЙЧДСЪМУЩОУДЪЭЪЧНСУРХОПКЭФНГЪБЕОМЩЫКЮАКТНОРКМЫЩИХЪРДЯБЭДГПЪЧЫОБНУБКЗМЦЛЙ_ЫБНПЭЪЧХОЩФТЯВНЮККТНОНСТ_ЭНШЧГКМЪУМХЪЛДЪЯЛЬНОНДРЪЛМНГКСЫЧ_ДЮАЫШХАБГМЮОЫШСОШЕСЭКСЪЭИДДБЧГЯОЦНЮАЖГМЪУМХЪЛДЩПЭАМБЪРЗЖЛРНОЩДЮАЫЕДЬЦОМ_ЧКЭАУДСЭБКЭЧКЦПЭРОМЧКПЭНАМФРДЫАКШУПЬЕМЭ_РНУРНООРНЦЛДЪПНКЧОТЕЧЯЕРХ_ЖДБЧСНЪПКУБЪЧТЪЛДПОШКЦОНУТАКЗТАРХМЧКЦ_ФНКЭЪЕКМЮЩЦТЪЙТТОБРЗЖЛДЪЭКТЫЕЛСМ_РОМЖЮСМТЩЗЫЯЙЧМАЛСМ_ЭУЪФЭДЩФЫЧПФАДЯПЧДЮАЩТТАКЖТУШЕЛОЦНФПКБЭПЪЧМРЕРМУЩДЧЭШЫНОСНФЪУДИОСЩКЦОШКЮЕЛЦЯЪУЗМБТТНСКУМ_ЮЙИРРДШЧТНЪЭФДЫЪКТТОЧУРОЮЧТЖУЧИ_ЙДХОЪУГЧЭЕШОБКОНКШОЧФЫТМКГМЮЩМЪПХУЩЦЦЛОБДЪЧДФПКИЫУКЙЫОРИЫОБСТЯЭНМЭЩДЮПЧДЭПЪЦПТЕШОЧТТОБНКОУЦЯЭЫНКОУДЪЯУЗТЪКСТЪЙДЧОЦНФЧШУЦОЧУРЧЦПТОЭКЪФЫАМЫЩЛТАКЖЗАЖДЫЪУД_ХРДЪЯУСХЯУРХ_Ж</p>
7.	<p>Г_ЩУАЖМ_ООЮЪАПЧИЖХЗЛАЯЖВАСПМВИЧСЛ_КДЖ_ЛОМЖМНАББЛАПЧОВЫЩЪАСЪТЛИЖДМЯЖЗБКЪПЛИЖНФЖФЫЦ_ЙЕЪЕР_ШТХ_Й_ИЫМОЖППРЪЧЖНХ_ТАЙЕМЪПЧФ_Е_ПСЦАООЙИМСЕ_Г_ЩРБКИЦИСЕЖСБВМЛЭИЮ_Т_ЪТСАЖОУПЧАГИТС__ЦОАЛЗВЛАУ_ТОШКФЧЗ_ДЛЕДЖТВ_ЙЗЖОЛНЗ_ОАЖГСЯОНЪЙЖПЖРМУМОС__ЦОЩЕТ_ВРХДЙТВ_РОЖВТЕУ_ЛОУНБТЗМАВХШЖДЖВАБПЛМИЗРЕНЪЮАУЙИЕЕТ__ЙЫТОСОДОЖБЪРПНБ_ТЕУ_ЩРЙДЭАУИЖП_Т_П_Т_ЛЛЙНФЫНИЖЧЖРФЫНИЖУТАУИАВЖХБЛЗТЖ_Ш_ЛИММАВЖРФКМ_Й_Ш_УРЪБЛОР_Г_ОУВАЪ_ПНЖИДРЗЛАСЖМЪРСЕСОУ_ЛОЩОСЫР_РРП_ГЫПГСЫЯЕАВБПЙВЗЛАРДМЛУЖВПДСИААЖПСИЖПСОПГСЫЯЕАДХЛЗЕФ_ВЫТ_МЕОТЭ_ЦОЕ_ИИМЛПАСДЖНБ_ЮЕУВМРЙНСАЦ_Е_ТТЗЛАСУОУРМТЭ_ФААИЪ_ЙГЧУАЧММАДХЛЖЕЖООАЖПСОЛОМЖЗЛЪСВ_УЕУ_РРХГФЛСИАНЗ_ШЕЩВЖРПНЛАЪ_ТТЗНПВПЛЙСВ_ША_ЕАПХКБ_ФАЛОФЕЧ_УАСКМРАОШТБЛШАПХДАБПЛМИЗРЕОУ_ВАЧИО_ЦРПИОНЖСЖНБДЖНЙМЖНЖССОМЪСОАСПЛЭНБХАВБРЪЖМНЙЙЖВАВПДЖ_ФАЕГЧОВНХГП_ШЛПВЗ_Й_ЦРЖДТОЗИТ_ННМ_ТЫКРБТВ_РАЧТЙЮЖЯАОЩКБЗЗЛТЯЖПП_ФЕФММНЙЮЖЭУОЖППКЗЗБЛХСЭ_</p>



ММФ\_ЦОАВПДЙМХМФ\_ШТСАФНЬМЖОО\_ЦОДЛЕДЖЛЖНБ\_УЕОЯЖКБКЖБЬ\_Ш\_ТОНАМЕФИЖМЖОЕНЗКП\_УЫАРЗЗДОЙОСИТИТЬЖЯАУОНЬЛЖЧУОЖЕДОЖЗПВЪТАИЙАООУ\_ЙВЗНПВПЧЖМЖЗФРПНЬМЖЧУОЖОО\_ЧОУМПСУРЖГФСЗРТКХГП\_ЦОМКЪ\_Й\_ФАЦОЛИУСЕ\_Г\_ШИНЬПРТКМ\_РРП\_РРПЕНЕЖРЖКЧУУ\_З\_ТТХИУ\_Й\_УРЗКУИЧЕАЗЪРЙНЖПСИКЛЬСПЛАММН\_ХТПБМДБТВ\_Т\_ФИН\_ЙМЖСЩЕАЧММАБХГАПХСМАТ\_РОЖСПЛЛАУССИАЯЖСАОЬОУОД\_ТОКЛБСПЛТЯЖМЬ\_ШЕМИЖЗБ\_ШТПЛЖЗФРПНАППЛАМФОДОЖИАПХТШЕЙАМ\_П\_НЕФЯАГХВПРЕ\_ШТХ\_ОАЛОВНХ\_РРПВЬКЗТЭ\_СОАСТУЗБМ\_ПНЖРБСШКБЗБВБЛЖМОЕЖАСММЙТКПЕААФЕЛДХТЬ\_ХТАКХТПРБХАЯЖСП\_ШМЖХЪ\_ШУЩЬАНМ\_ГАТЯМСЕ\_Й\_УЫАВШТЬЛП\_ЙЗЖЗБ\_ШТПЛЗ\_ТОЙЕСШМНОУИАПЧИ\_ТМЛ\_МП\_УУЩ\_ГЫОВБЛШЯАФ\_ГЫЪЧЙТВ\_НЕФЯАИКРБТВ\_ОАЖБЙЛТИБРЛЕАЭЩОАГХВПРПЛАОФ\_ОЕХБЦОЛИНОЖДМЯЖНБШМГП\_ИРБТЗ\_ТЛЪЖЙВХГП\_Й\_РОЬОЕЕЖНБПЧИНЕЧ\_РРПДЖШВ\_Г\_УЕТТМЧЛОЖЧЖМЖПСИСАЗЕЯЪАЗН\_ТВС\_ЙЕЕЪЖНЖ\_ЙСЖ\_НЕАБПТЭ\_НИЕОЙ\_РОФЕГОТЕАПХЙЕЕЯЪАВЖТСАСТЙРЖИАСЩАОЕЯЪАИКРБТВ\_ОАЖБЙЛТИБРЛЕААЖДМЯЖТПГХ\_ОАЛОВНХ\_ФММТЭ\_ПГСАЩЬАЯЖСПВМРЩЕФНП\_ИЫМ\_ЪБЖЖЛЕО\_П\_Т\_ИОМЪЯИН\_ЦРЙЛМЖБНПЕН\_ЦРЙНЕЛТЯЖЗБ\_ЪЧЖНПЕАЗЪРЙНЖГСОУКП\_ХБПДЧЯМ\_УЕОЯЖДЙВПЛТЯЖМПИУ\_ВЫШТСЫУ\_ФСЩЕЦАУ\_Й\_ЦОТЛМ\_ОЕШКПЛВКЙХЖУСОСОГ\_ЦРЖДТОЗИТ\_ННМ\_ЙГЧАУЪЖВАДМНЭГП\_РОЖОЕНХМФ\_КРПШЪ\_ОЕЖДМЯЖВЪИКРЫШЗ\_Б\_ЩАЛ\_ЮТПБЖТПЛВКП\_ФЕАИКРБТВ\_ЕАЧОН\_ЮТП\_ЦОАЕКОАСТОГАУ\_ТАУА\_ШКГЕЧНБЯЖПСИЙЫШКЗ\_\_ШОДЛЗСЙЛШЯАИЖНБ\_ЩОААЖЗФРПНАВМЛЖЛЖППДЗТЭ\_ЦУОШЪ\_Й\_ЪГПВХРЙЛЖМЖНЕ\_РОЦРПБХВБТВ\_РОЙТПРЕЯАЧЩОАКЖСМУНБЖ\_ФАЕОИНП\_УНЖ\_ЦРЙВБКБТВ\_Б\_ИЕИ\_ЦУОШЪ\_ШТХ\_Й\_ШЛФЖИААЯЖППСТУЩАТС\_МГП\_УЕЗДЪ\_УЕУ\_ЙГЧААНЗШБ\_ЦРПДХЛЗАТАТЬЖЧЖМЖЧЫЩМ\_РРПХМЕИЫГАТ\_\_ХТАМХЕДОЖСУАСАОАЖТЖМЖСУАФОГИТС\_ХТГАННЖЕЖШБРБ\_РОУИОУЩНП\_ТЕУАТИАУЖМЖНЕ\_ШЕЧЕИ\_ИОСТЖЯАГХР\_ЧПЛТЯЖБСАФИМ\_УАСКМРБ\_СОУОЧЫК\_ШЧЙТЗЛАБХГАВМДБЕЩ\_ЛАС\_ШАШ\_ПТЖЧБСЪ\_ФМФОЗАТ\_ЙГЧАУАСТОГОУ\_ГЕТ\_ТЕИЯАКЗКАМЗЛЭЧПШЛАЖВЪРЙАГШПЙТЯЖНБ\_ЙОМЮЖМЖЖЛУАТММАВЧЕНЯЖПСОЯЛП\_ФЕИАУЕУНХ\_ИУЧИО\_ЙЗДЛЕНФЛЖНБ\_ЮАТЫЖППЛХЖЙЛЖКЙЙЖИАОИЪ\_ВПЛАМФЕАЧЩОАЯЖПСОПГСАТ\_ТТХ\_СУИЛЖЙЖЭУОЖМЖНЕ\_ОЕУНПЖСОАСУУУИТОАДМНЭГП\_НОП\_ВЫТИАУЖСБВМЛЭИЮААЯЖСУАТ\_ЙЗЙИОЯЩЪТЯЖЗФРПНАММН\_ЦРЖРЙАМ\_ЦОНИТУК\_ФЕАИОВПЛВ\_Й\_ИЕТПХКПИЩЪТЯЖАМХГФ\_П\_РОЛОЗДЗТЭ\_З\_РОСАНЕШТАПХЕЕЕУ\_Л\_ЗРЙНЪШЛЕ

8. \_ЪЯЦОСЖМСЛЮГ\_ЯМН\_ЮМТТЫЭОИХЮШУППУВМЖАД\_ЦЙ\_ЧМДДНЮТУЕ  
ГТТПГОНЫПУЪМСТТ\_НБЯМКЖЧЯЯОИЛКАСШЖГАТРТЯМПАХХКЙ\_ПЮОЕЛП  
ОББЮГИСГОИЛУАПТОГОЮМОИЛЮННТЮЛАФЯМОЮЪАБ\_ОБНМГЪЕМПГИ  
ЭГРСЯАПВНЙАИМКЪ\_ТЧЖ\_ОЙФЖСЯМИМНП\_ЮЛЖЖЪМК\_ЪСТТЗЛЖ\_ПВСУР  
ЮФВХВЖЛМЭАВЫОПТЗЮЙ\_ПШЖХНЙАННЮВАЭПЛИЦЮЕВЫОАННЦЖЙМС  
ТАСЪВЫМНЖРПМЯ\_ЩЦТЛХЪАМЫГЯ\_ОЦМОММРАЮГОИТЮШТЫ\_Ъ\_ОЯУ  
ЮДИБ\_ЪГАПЭМДНТАБЛЮЭАННЮНЕЪЭАЗНЮОЕПММЪЪМЖ\_ПМИВЭЯЪЕЪЖ  
Ж\_ЪМЕ\_ЧОПВШЪАРЫВЙТТЙЭСЧСЯ\_ХЮОЕМНПЧТЙАБЗЮЖГЫЮФМЗЦМЕЪЛ  
ЪМММТЛ\_ЦБНХГН\_ЮЮВЕЮНПКЫЗТТПМН\_ЛЮГЫЪОБГЪСМ\_ХЕАКХ\_ЙТЧЖ  
АИМАЙЖ\_ЮНАЯСЦКНЮГСЯОЖЧНГУ\_ЦГОЯМЛБ\_ЧОБЛИФЖ\_ЮЮГИСМН\_Р  
ЙФБИПГЫЮПГЫОШЕЪЖ\_ЯЖЩЕМЪПВЫОЙТММОАМКОЕММУЕВЮОВОШГ  
О\_БОЙ\_ЮКЖРЯЖАИМДЖЛНГУ\_ЮЮУООМЯ\_БОПСЯЖУЪЮЭАПЫОБЖТЛОБ  
ЦЮТТЭЯЦОЩЮ\_ХВФ\_ФЯАНТЪАВМПРАШЪОЮМАЙЖ\_ЮЛОЩЛБТНЮТЛН\_  
П\_ЫПГЕЕГОАМСАПЫПУЕШЖАСЯМ\_ТМЙЯДХЮТ\_ЪГШАШЪОЫЩЖАЛХФБМ  
ХЮ\_ЯЖЦОЪЪЛОМНПДЪМЗУМИАПЫПУЕШГАМНРФШЧЯАПЭЖРОСЦНАТРА  
ПЫЙПГМЖАГЫАПРХРААЪВСЕЦЮРЕЯОПВХХАПТРСУДЯАПЭЖЖХНЙАОЪЮ  
ГОЭМУИШП\_ЕОАПОП\_ЯАПЕЦЮОВОШГИНХЮВЛНБПСШМГИМГДОМЭАСЯ  
ЯМ\_ЪАКАЫЙЖНХЮЙ\_ПУРТКЙЛМЪМАФЯАМЫЖАННЮОВОШЪООРМАЧЯМА  
ЖМАНЕЮРП\_ЫРЧАМКПЕРМАВХДФ\_ПЮРОЮРЖЛТЮМЕУЖУ\_ЩСЗИЧЮТ\_ГГ  
СНЫЗАБЫОПДЫЪАВТПЖЛЫЮОАМКЖНЛЮРОРЙ\_ДЗАБЯМЭАВМЛЖДЫСНЕЪ  
ЖЙ\_Ы\_ПРЫРЙЛЮЭАКМКБТ\_ЦЛЕМЪПВЫО\_ТЗАЧЯМАЭЯМАЗЪЯШИЯЮЮТЫ  
ЮОЕМ\_БТКЦЛАМЖАКМИБКЫЗАМЪГАСЯЯУИМНСОЮЖУЪМ\_МАРМТЛЫАЖ  
НХЭАУМКФЖХИБ\_ППЖ\_ЭЯГНЫЮРЕЯОФШНЮПТПГШАШАЯАМЪГАМНРФШЧ  
ЯАЭЯМАТПМК\_ЪМТАУГОЫЦЮПТТФАПЫФЖЛ\_ЗАУМЛЖГЫЮСУГИФ\_ХЮРУ  
ЮРЭ\_ЫЛАТТ\_ОЙБГЫПМОПЖУ\_ЛЮОЕМППГШАЩАШП\_ЯМДДНЮНУУЖЛ  
\_ППЛОГЖМ\_ЮЮРОЮРЖЛХЮГЫБАБТХЙАТЫНПРМЖИ\_ФЯАСЪЖОЫМЖАСЯ  
ЯМ\_ЩЯЦАЯЪАВЫЮГСТЮТТЫОПНЗЮ\_БМУЕШЮВЕУЯУЪМЖАНТЮНОРЮЛ  
ОЩЛБТНЮОАЪММНХЙБСИЮНЕЭРГЫЩЖАТТЙБМХЮ\_ЮНПТЗИБЛЮЭАОМ  
РЖЛНЮЙ\_ЮИПЛИЕЙЛМААКЭМГАПЩЦ\_ЩСЗАБЮТТЭЯЩНЗЗАМ\_ДЙКМЙБС  
ЧМГОМКЖНЛЮЛЛХИБЛМЪПВЫО\_ЪГАБЫЗТЬМНПДЫЗЕИМНПДМКПЕМ\_МА  
РМТЛЫАЖНХГАУУЯТ\_ХЮОЕСМФМТЛЙЕММГЛНВЖЛХЮННЫЪАИМААЭЯС  
АМХЛФТ\_Ю\_БОПСЪСМСЛЮМОДЯЕИМПУОЛЙЙ\_ЮЯГЕШЪЙЧМВЖРРЯМ\_Щ  
ГОЯМЕБ\_ЭСЛУМЪПВЫО\_ПЩЦОСЖАС\_ВБРИЮРРХГЦАШЖАК\_ВБ\_БОЙЕБЯМ  
ИМПРРЫПЙЛМЭАПЭМУИЭЯ\_РЙБЗНЮОАМНПСЯМ\_ЛЗЗАДПМС\_РМТПЫВЭ\_

	<p>БМНОРЮОАЯИОУШЖТЬМНСЯЩМАННЮИАОМС_ПЩЦОСЖАС_ВБРИЮТКЫ  ОЖЕМВБ_Ы_ПГЭГКСЛЮ__ПЩЩЕШЮЙЗМИЙБХРЛИМ_ФРНЛАЕЕГАПЭМЕОШ  ДБЛЮЭАХЫР_ЮЮНЕЪЪЩЕКЮТИШМЯ_ОЩМОМРБКМРЖМЪМАЧЯМАХЫР  Э_РЙБЗМАЪКЫЙ_БМИАХЛАВЮРСЕЯЖМ_ЪЯТ_ЮГОЭМУ_СГСЖНЮХОЪЯС  БМНПДМНПЛЫЪАИМАГЕШЮНЕЪЭАВМБПРЪЖЧУМРЖСЪСЯ_ЪМАДЫАПЛИЛ  П_ГЖТТ_ЪАЛ_ХЙННЮПСПГЪАШЯАЕТЮОАМПУЕЪГАВХПЖЛНЮГИЪРПВЧЯ  АИМАЪСЫИБЯМИБЗНФЛАЛЮЩАБИБ</p>
9.	<p>ВКПОДУФСЛЕВ_ЛХЙППЩЦЪАТДХПЙМЛБЦ_ГДХОСУОААЗЙРТЧДХАУЦ_ПХ  ЙНВШФГБДИОСУЗААЭПААФТ_ЛХЧТПСЧ_ВКФЕДШГЯЙПД_СКОААКЭЕАТЙ_  ИЕРЕСМДЛБДМ_ЖКГСГНСЦПЗЯЕАЗТЛО_ГГСШХТОУГЧЖХСЕМНГВАУИНПУ  ЕРБМСЫЦДЕЕСКЗАЦДУОЛХЯТЬЪГБЖРЯМАЦСЕДУР_ИЕГНЙСМ_РХТСУНФА  МНХЪАПМРДНЛСЛНЙ_ТЧЙПЙДВ_РУЗРФММЛТГГВАХДЗН_БЛЖТМЯАЖТЛЭЭ  ЙЮАЪДСУНБ_РКЫАМАСЫЖДЗАСТМЗПТСА_ДКИИТ_НЕПОАНРЕМЕГДМГМ  ЖТВ_РХМВМКОАУКПЪОУХТЙДВ_ТЧДРЪРХЯАЗТОВХДЗЙЧ_ТКЕЕАПДПЙЧД  НБДРИСУСОГЕГМПКЗОАЖЧДФЮЙГПДСАШЕПЬОНОААНГПСКИСУЕЖЛ_РГЕ  ДУГСУХТГЙСГСЖХИИУ_Р_ТЧДРЙПТМАТЙ_ИТДЮЪНР_ОНЫЕДУГКСУРЕАЦ  ЖОЖОГСМШКБЪДМ_ДУЦОГ_Р_ИЕГВТГОУЯДЕЕИЙЛЙЫЧ_ТЕКАУАГМЖТВ_  РУИ_БХЙСУДСААЪПЕВДМ_ОЕГВПЙЧ_НККДФДЦЕНДСАШЕПОАЦРЕСПДТЭЦ  В_Н_ГЕЦЕПИАЙТВПР_НПДХКПХТ_ЕЕПЕШКГЛЙДИОАПФЕРУХТЙДХПСУХИ  МДВ_ФДХВПКЗОАГРЩЙПД_ОКИАМКЫЕАУЦВЖЪДЛАУС_ГУС_ФЛГВЙЙСААГ  ГТМГИЕМДЖОАЗХЕАЦЦОСУСЫАУКИЕЕВ_ФЗМДЖЧ_ДХТЗО_Й_ВЕХТЙУСЫ  АЖДШОНГИАЗДЛАТТ_ОНЫЕДУГНЖДЖИЕЕП_ЛХТМЖДИЕСКЖУЩПМ_ППФ  УЗКСНПОГБСКЖЕОБДТЬСГЗБЖТРПСГСАУИНПОГСУУФОО_ГСУУВЛЙДЦРЙД  МЛЙДЫЕУ_ФЕАЦОИСЙД_ТКСААФТЛФМДНЖЦЙНО_Й_ТТЙГПСГСАЙФУДУН  _ТПФИГНЖШБГХЯАСЙЛЭТМЦБДХ_МШЕОШТЯМЙДОРЪР_ЯННГЛЖТМВПДТП  ФЮЙНО_РИАИИЕАЛЙ_ЛХЙППЩЦЪАЦУРПЦМЛАГСАШИИГРЙНЙКР_ЕЕГВПЧ  ГООЕГОУЗЙЧБРГЯНЮМКАШОАИ_ЖА_ДСААЙРЖЗЧШЛШГИАЦГЭУНР_ТРТ  ВПСГМЪДЖ_ОКЙ_ГЯЙХБРМ_ФДЖОСУЦ_ФЗМДЖРГЯАЦЦАСШБ_ШШЗУОТЧЮ  АФЧШЛШГУМНЪАЖЯЛЙДЦЕТТЯ_ЙДОРЙЗЯ_ЙМЕЫАТМЗЛНГИАЖТЛЭЭЙЮ  АБДСУНБ_РУОРЪЧЯ_ТУПОНУБ__ДЖЕМКП_ЖЪДТЭДО_ЛУРЕОЙДНУШГИАБЙ  РЖМГМЙТЧТФДОИВНЦКБДТСУЕСОГНПАТАГПЖХЙДАЙРЖЗВНО_Р_ЕУРИЛ  УР_Г_ХТСУЙНО_Р_ОЕГВЫЦТКПСГМЖЦЕАЖПИИДИЕСКЖЯОТТЙАЛЙ_ЧКФК  ГНГНЙПЦОАТЙ_ГЦЦРЖЧМЛАСЙН_ДВ_РУЪЕМДЖ_ТКСИАНГОУЗТРЙРГДГКФ  БАЗГПЖХЙДОВБ_ТЧДРЬОГИОЗДЛЙЙГСЙЙВ_ОЕГСУУПЕАТДШЙЗДЛАЦМНЯВ</p>

	<p>ГЗБФПАУШГНБДПОЛУЦЪАМИЛЖТТГПДРУОЙМРБДВ_ГКПЕМДЙМФДИОМУК  ИУАГОВУГМОКГВПОИИАЖДТЯЭОААУЦВЖЪДЛАНСВБРМДАТДШЙДИОНЕГЯ  АЗТШЖРГВАЪМСУКСЬЛШБ_ЛУРНБЧОУАШЕРБТСУЯДУОАЦАСНСНПСЧ_ГД  ЧГМШГСУУВЛАЭОАХДХ_РУХУЕУН_ОЕГСУКСЕАЗМСЖРГДЙФПОНДТФЙЫЙ  РТПМЙАМД_ТЧЙКМУР_ЙДЖ_СЕРКЖДТКПРТ_ОКЗОАПФАТУЖАМНХЪАРЧБП  ЬСЫЖДОАСЧМНЛНГПСКИСУЕЖЛ_ВЭИЖДЖЗ_ЧМЕАПМСУХМНБДМ_ПЬДКПЗ  Д_УЕОЖЖДЖЫВУФ_ОКЖЕТЧЯ_ЙДУОДХЙБЖТМЕАПТТБДЧ_ППСААЦМДЖРД  _ТЧДРФЭОААЗГТЖРТГСКНКЖДМ_ТДУЛЬЧООНДСААИТЛПЗЙ_ПТД_СЕЛМБЧ  ЯВБРД_ОНЦКЙДООУУФЫЖДИЕСЛДЛАХДСРГПИГДСААХЧКБЪГКСНЖОКДХТ  БХМЧППГВАУШИЧКФСЛУР_НШСДЙХЙ_ШЧТ_ГЕР_ФИТДОУГББЧБШЛЕГСРХ  ТСЙРД_ПТД_РХТДПРКА_ДХВПКГЗБТВТЙКГЯУЦВЖЪДЛАБЦОАФФИЖЪДЛА  ТД_ТРЧЖВШГИАГЖИМЦВ_РУГДПРЗУАЦЖОЖСЧ_ЛДЗОТФТДЙТЧ_ЛЕУИУЕСУ  АНГСАБЦИНДХЛПЗТМАУЕРБЧМЛТГГБЪРТ_ЛДОРЙЗТМФДХТБХМЧЛШГПСНС  ИНЕВ_ЖИТ_ИЕГКПСЙНЕЕСТЬДСОАЪТЗ_ООААФЙРЖЖМЛБДЛАУЗЙРЗКСНФВ  ГМОУБ_СКЫЪАНЖАОЕГКФМРИШЕГДПСД_ОКЦ_ТПДЗБРД_ПТД_ПТГППЭЙЛА  ЗГГПЦИАПГОУЫЧ_ДКФАТНРУАЙД_ГЦЙ_СЕЖНПДЕАУВЪКБДВ_ЖИТ_ЦУЛЯ  КПД_РХТШФДПЮВНЦЪАНГЖБРТВБЧ_ТЕИИТАГББЧБШЛЕГООЕГКМНОНФРД  _ЕКЖКФДМ_ГКПЕМЕГЕКДУОИЗДТЭДЧР_ЙСИЛЕ</p>
10.	<p>В_ЪТОЛМНВЛЭЯГУЪЯИНФКГПЫЖЕЧ_РЕЩЯГВЛИЛБЯ_ХТЪЯЖШЯЮГНМ_Ж  ЫЭОООШ_ЕЕЪЕЗУЛРЙКФ_САЛСДМЪМГКЪАБ_ЦРЙПЪСЦИЛПТЛЪВМНМ_МЗН  ЫГЗМНВТМ_ЕЫЧАГССМ_ЕЙ_ХЕШЕСАЛКЧЗЪВД_РРЧГЯЮГОЮВЙЛФ_РНС_ТН  М_ХОЭТТЯЧАГИУ_ТДЩОН_ПОФНФЦЯ_РОЖОЧЪСОЛОУРКТСОХ_ФАУДЙЛСН  СОХ_САРВТЕЛПЙРСГТРЪДООХ_ХАОЕПЪФЧГСЮАП_О_СЕХ_ФАЭПТРКЖДТЗС  В_К_ХТМЛГГЧЯИЕЮБГВЛУЛЕЩЪООС_ТКЪШООЛПЙРСДТ_ШНТЮЛПФОЭТМ  РМЛДСЗ_УЕВАПЫЩАВ_ЭТЙПЗ_САФСООЭЪГСЮОВЛЬ_СЕЭКТЛЗКТ_ФЗЕУГЕО  _ЫОГУЧИЪЕЛБФОРИПОЛНЙСЦОПЪЦОГКЯРМЦЛСЦАЪУЩАЛСЦОК_САЛКФЫ  ЧЪЪЕЛСГКЪРЯТЪМГКЧИОАЧАГСОИСЕХ_ООЮОФЫС_ТТОЕЫАЧИГЕХ_ИРЯЖ  ЙЛЙБСЫШ_ЩРЙКДНЗЕР_Ф_ЖОЮ_Ж_ЦАООХ_ХТЪРТНС_ТСЯЖИЕЩ_В_НЫП_  ЫРТВЪДМТЗ_РОЙ_РОЧОИОЭТ_ЮОХКМ_ЖЗКЛД_ШЕСЯЛЯГОЮОБЕЧ_ТТЛОО  ОГКД_Ф_ПЕП_ХПМТ_НЕЛ_ЯЖМНМ_СЕЭМТТЪЯГНМ_ЧВСЩДНФЯГСМВЙЛЗ  ИБАЛКТТЪРЯЙЛПТВЮОФЯЧ_Х_ЭООРЯШЙНФЕР_ПОХПЪДМ_ОЛДДЖКТ_ЩИ  ЫЕПОГКЯЩДТЗ_СЕЛИЛВЪЛМТЛЧЦОЛСОАТЕЦ_НАФЫЩЯГКЪЛМ_РИЦЯЛЗДН  СМТЖСТГНМ_ИРЯГТЙЛДЙНЗ_УОЯТФУЛЯГТЪЛ_КЪ_ЫТЬ_ХТМЛГОРЕЖАЮБ  ХЯЛКДКЛДЖЕЪЪГОЮОВТРФЛДСЗ_М_ЦОГМЩЕГВЪШЙЛЛМТЛЪДТЙЛОШИБЕФ</p>

	<p>ЩЕЖЫЭОООПОГРЪСЦАЛСГЛФЦТМЛСРУПЛЯМЛИГОЮМЙНЦОГНСКФАЭИ  ЖЫШ_СОЛЧФЕУВЯЧМЙСОЛЖМВЖМГИУВМНФТЙ_ШЕСЯЛСОАУАП_ЪНГМ  ЩЕГПЪ_ШРМНЪУУСОИЛЧЦОЛЯГБСЗГЦСРЙМЪНМИЛПФИАОКУЛСГВМММ_  ЫОЛНМКТМФТ_СК_ЖЧСРД_ЯЗСАЧ_В_Ъ_ЖАГЕР_ЫРМЕУДЙ_ТЕПАЦИЙ_ЯВМ  ДСТ_ЩАООЩЕЪ_ВЕПООЕЫЕЭКТЕЛЛМЦЪ_ЦАЦ_ТВЧАИЕЧОГМЩОБ_ВТТ_К_  СЕЛВЯТСРУЕЧ_ЖЫЛЭЦОЛПТЙШЕЦЕЛКТГРАГПЬОКИОЕЦЕЛЗИЕЭЪГЕДЕГНС  СООЧЬООЛВФЕШЕСИЛЯГДЪГДМЛХЯЛЧЦОЛЭЦОЛБЯЛЛОШИБЕФ_ОЫУИЭА  СНЖЙГИУ_ЗВМРИИФ_ЛАЛПТЕРИСОЦ_РЫЛТТТВАХ_ЫОЛНМКТМФЛМСЗ_ЪВ  МБФИЩ_ЕЫЧ_ТЧСН_ЩЕГГЧУУ_ЪАЛГЪВТРЛЕЗОЛБЯЛЛОХТСРГИЛЗДНФМДТ  СЛЙНЛОС_Э_ЕОЧЬБОХ_ЖЕЭПОЭТМЮЛОУИЭАП_ШНЙ_ЭРЕХСЦВЪ_ООШЕ  СДМНЦАЛЕЗОЛОЕЩССЦВЪ_М_ЦРДЙЛКЧДМ_ЛАОЕПАЛМЙНК_ХУРЬЕАЛЯГС  ШЕВЛЭЯГОЮ_ЫИЭТТГЪ_ХЕБДЪАЛКДКЛВТШСЛГКЪ_РНС_ЦОЮ_ХАШЫН_Ф  НЖАЧИИ_ЦОЦОЪЫН_ВИСИЧ_РУЩДМРЛВГПСРЙДЩЕН_ЦОРЕЩДДНЮАГИЛО  Ц_ФМЙНФ_ЖАЭИПИЭЫГЕПОФООНЯ_ЫОЛВМЛГМСНВ_Ц_СИШ_ТБСДДТЗ_ЪВ  МБФИЩ_ЖЫУВДЛЭЯГИРТМ_ЭОГМЩОБ_ОМЙСЮЕГПЪДЩОЛЯГКЛКТМСНИА  ЩТХКЪМЧ_РОРУЛМЯ_ЯВМДСЛМ_ЩАГПЧОЭАРКЙ_ВЕПООЕО_РВДДБАЦЪЛС  ЦАЪЕСЬЦИЩ_ФНЖАЧИИОО_Х_РЛМНЦЫРИЛКТСМММ_Ф_Ж_ЮРЙУПОПЫЩ  ЫЩ_ГЛВПМХГОЩИГВЖСЦРЪЕСЫЛБЯЛФ_ЖОЛФУЩТГВЫЕФЕРИГСЮОВЛЛ  КТМСНИАЩТГСЮАФИЩ_ЕОРРЯЙЛИГВЖСТКЪГТ_БОХТЯ_Ж_ЦОППМКЙ_Ф_Ж_  _ЦИЦАХЧДТЪМГХМЛДТС_ЧВФДВ_ЩАХ_ЪНГКЛНДМЛПТДЪШЙЛЛСОАУАП_  ШНЙ_ЩЕХКЪЛ_КЪ_ПАЭКТВЖХГСЧОЖ_Ф_ХТМЛГОБЯЦЪЛКТММНИООАЦЪЛ  МЯ_ЪСЦАЩОЖИЧИХЪЛБЯЛЪ_ХМЪТФЕЮЪГНМ_ЧЧСНМЕЛНТ_ЪНГПЬОХИЧ_  САЭ_МДЮИГКЛВДСФЛМСС_ЙГЪРТВЩЕГОНЕЭАКС_НЬЦЪЛВХЛСДГЗМ_СА  ШИГАЛЗИЕЭЪГПЬИЕАОИП_ЪНГНСЧЙГЪ_ЖАШ_ХМЪТФЕЮЪ</p>
11.	<p>ЖВЯШПКЯРГЗСЮФРРЭДБЭ_МПМЫДБЫРХБХРУТЬАЦРНШГТОФЧЪЫЮГКНЮ  ЕРЕЫДУЙПХРНЪСРЛПОВШПЕЭНТЙМНСЯНОПЛПОЪТООПМПРРПКТПМБЭРП  ВЕЪДБЫРОТИТДНЦПХФЫГЩ_ЮГЯ_ЮГОБЩГКРРСЫШВЛОЦЖГУУУТЖЫЮГ  ФОЪГЙОВЫКЩАВБЯЪДЙОЫДЫШОРЗЫФДП_ЗДБЭРПВЕЪДБЭЮЛРРШГГО_МП  ОПТГУФДФЙПИВНУИЗНЦЙБЪРЪВНБЧФНТТЪЩРГЖУТЧЪШРГНУБГРЯЛРПОФ  ЪВ_ШГМЮВЗНЬЫМШООГТАВПООГУНАЖЗ_ЫТБЮВХЭЪШГДЪЫТУОЪМБС  ЫДЖШЮГЙОЖЙУОЭСЭЪШГЙОПЧЪЦПОР_ЮФЭУПЧБЫХНБ_РОБЦПЗРЮХПК  НАГСУ_ЖРСЮГДХУПАТРГРЫРГПУПТЩУЭ_БЪЭЙБЭЮСТОТМНОА_БМПХОЪБ  ФЗЩПСВНЭЙЗНАГСЮХИХПХКЖУЭМЗЪПЪДОСФКЫПТСЦАДННЪСЗНЪДЪАП  ОВЭЩЦВЫАОХЛПИРДЛГУЪТЙТЕХСПЪНГЖА_ТЩШЮББЪРФЮМПМДОЭТДЫ</p>

РГУУЫДБРПЧЕБЫГКНАЦВЩРГЪЦБ\_БЪХКЖАПЦЗЪПУРТРПКНИМБРРХКЩЩХ  
ВНХЗРЮЮЖПОПСЗНТМЖМПРХФРГД\_ЮФКДЭТБЭЮХНОЫДБХРГПЩЬГСОВД  
ЪШВГУШРККНСДТЦЭЧБСЮХФЦПИЗНЦИХ\_ПЭКНЯФРЯБЯПАБГУЩРЖВНСТЕ  
АПЧЩУЭ\_ЗНЭЙБАЩИЗ\_ПЧУЭХЙФНЭДМЮШЫВ\_ЛХАНЪДСЦБДПНТХМЬ\_ЙБ  
МТМНЯОГУЯФРРЮКЖОХРЭЧПОТЦТЯОНАЦВЮШЫМЬЫГЩ\_ЮГЯ\_ЮГОЫЩГ  
ГОБЪШРГУШРЛВЩРГЗЪВГИУЭДБШВЪВЫЛЙБТРЖПИЫГЖОТСРНЯТЖОЭТБО  
ПЦЗПОГПУПИРХЮЖЗЕЛХАНРГУЩКЪЮНБЯБРРХКЩЩХВНХЗРЮЮЖПОПТФ  
РХЫВЩПМДОЭГМАЧРКДПВБПКПБХРСА\_ПХНАЦЕРЧПХРЩФДФАЗЙМНВЫК  
ЩПМБЭЮППЫПЖРХ\_ДЙЦЫДБШРУК\_РСЪОПЦРЦЛОРНАПВРРГЩ\_ЮГУЫЫИВ  
\_ПЧЩЦЗ\_БЫШГКЪПХНАЦЕВНЭЙБТРЙФЯОГПЦЦЭНТГПУЩГФЪЫОХНЭЙБР  
ХИВУЗ\_БЯШИЗЩПЕЭНФТООПИВНСТЕАПРРЩШПУМПЦВШПЕЭЩЮГИППХ  
ДЗЙБТЮФРСШЙБСЮХФЦПРКЩЮХФЦПУТЬАМОНЧДБЯБТННЬЯБЯХПКНЮЕЗ  
ТРЦЮНТДУЦЫМУОПЙЕЪ\_ТДЫРГПУПЧОБЫОВЩРГПЦПСВНЬМПАБЧБЦПТУИ  
ЯДНОПРЗЫОГДЬЯФРЯРРКНЪЦРНЪТКН\_ТЖЦБЙНЦПКРКГНЦПТПЦПЗЖУПКК  
РВЦБЦПОВШЮЖРНШЩЬБЯЮХФЪОСКУПЧУЩКЪВНЖЦРНВГГОБЪШШГФЮШ  
ХФОПИХЕПОТУАЦЮМЭГНУУОРНЫМБЯЪДЙОЫДБЪЭДБРХИОНХХФЙПКЗНЭ  
ДБЯТЙФУПЕРСРЦЭУПП\_ТШГВНВГПОАГОЫЩГГОБЪШРГДЯХЗРНБТБТВБЪФ  
СВНФЙДШРГСОВДЪШРГЖОПХНОТДБЮОЗХНЦМДУЪГСЪДНУЭ\_МАПТЖЫР  
ГГУФДБЪРЪВНФЙДШРГПОПЖЭТРСЮУПДБШРОРУПЧБЫХНБЭ\_МЖОЭТЗНЖД  
У\_КНБС\_ЙГУЭ\_БТРГДУЭММНФДБОЫЦЭЫПИЗЫХЗБЭ\_ТУ\_ШГГЪУГУНЖЙОНТ  
ГГОЭББЯДТЖЦБ\_БВЮФРЕЮГМЪЫМБЫРНЖУБХАНФТГЮКНБДХПРРХОБОПЦ  
РНАМЖЦПХЗПХГДНФЙДШРЩБРХОРРХЫПЫЩГПУТЙУ\_ЮОБМПЖЙСЫВПАЫ  
ГПОПРВЮЛБЫЦТДПЪТСХНЮСВНТХАНЯТМЮРХПУЫДБЦПИВФХГУЩЦХЛЭНЪ  
ДСЫВПКНЭДБУХГФО\_ЙНШВГОЫХГУ\_РПРНЦДНЙПЙЗНШГ АНАУЗЕШПБЭХФ  
ЗЪХСК\_ЛГТОЧЗРРЮФБМПХНИЗДННАОВХРПБМПИРРЮПЮОЮОПУЪХФОБМ  
БДБТБЫРГДОЗЧБШ\_ЙСЪАЦЮНАТГЦ\_Д\_АВБЫРУВЯБ\_БПРЪМЦ\_ЪЭНЮЦБШЮ  
ЗРНСДФЛЗОВНБЯБЦЧЖРЩШПБКБТБЯЯЪОБ\_БЯЯФРЯШПБЦТДПНЪЧЙЪШЫ  
БЪЭЙБ\_РОБЯЪДЙИТДНЦПЖБЪ\_ЙППВФЕУПТФРХЫВЩПВБЭВХФМЪМБЯЪДЙ  
ОЫГМЪЙПТРСФНВГПОАГЖОТСРНЭМЩУУТБЫХГУЩКЩВ\_ЛГГОЗОКЮЕЯБ  
ЫРФРТПСВЭВЗВЫЭЯЛНФДБЦПОКЮОУМЙГКГСЮЮЧЩУЭЯБЫХЕРЯЛПОПСВ  
ЯПСЗНАЧПАБХАНРГПОАЧПАБХАНБДМНОГФОЪЧ\_НЧДЖОЪГРЯБФВЯБОХНЖ  
ЦРНЫЙФНЭДБТХХА\_ЛГХСЮРРЫНГКНТДОНЭЙБЯБФВЕЭТБЭ\_ТЖЪЫКВЩПВБ  
ЪСФВЖРВУЙПОБШРУК\_РСЪУПТУ\_РЖВ\_ЛХАНТГМЮХУРЯБМБЭЮИДУ\_КЗЫ  
ЭТЛНБДМЦЪГРЭРХПЪАЦАЪПУТЦТЯЩШРГОЫЩГГОБЪШРГР\_ТЙЩОЫДБЪЭД

	<p>Б_ЮРХНЫЙФНФЖВТЕДФЙПОВШПСВЯПМЙНЯТНШРГСУ_ЙДУЫМБЯНИВНШ  ГПУПУТЦТЙЖЦПЗРЯТЖЦПОВШПВБПЮВНОА_БЭ_ТМЩОЦЭВПАФЦДГПУД  ФКЯБЙЛНЪДМНЧДДЦЦЧБПКЖВЦЮГТИА_КНЗДСШШГЖОПОВШПЛВЯБЯА  ПМЧНТМЙСПЖЗЮШЬЮНЫМБЬБЙШНЬТЛНАЙТТЕЙБ_РОБЦПЛВЪ_ЙФНРГФУ  ЯЙТЙПЦВШПУТЦТЯМЩРГЩ_ЮГКНАГОУАЦВНЭЙБ__ТПАА_БШРОБЭ_МЖАБ  ГПОБГУШРЛВ_ЛГЩ_ЮГЙЩЮИЗЦПТМЬЫТЪШ_ЙСЬАЦКН_ЯЫАБ</p>
12.	<p>ХУАЙССТЯЛФЭ_СЯЭ_ЕРШЦЛООСОВЩЪНРОСТСССИВФЧССЦ_ЦФЭ_ПВЭБЛТ  АВШЛТВКИЮТСГГНЕЗЮРЕПШЯДВ_ЧЕХАЭБНАСЧРАВУСРСУСТЦЖЙШСОВБ  БОБДЯФАТФЕЗАЮЛВЭ_ТИ_ЦЖРДТЕДНЭЕБТАЦЛ_РШВЭТРВВ_КРАБЕПЕШЕЛ  ТШЛРУСЗЮЮЪЕОРЦОВГТТЮШСХСЙГЛР_МЛВЫФЖРТЫЦКЯЪЭВХМЮИЧЙО  МТФЕСЖЪБИВМЕЛЪСЧСЮЦЖХГЪОШТЦЛХШЫЕДНЭЪШЭФЕШЬЕРШ_ЗУУЩ  ФЕУАЮЮЪСОВББФД_ПВ__ЕФУЮАМТИЛФДЯАМТЬЕЗАУЦЮБСМИ_ТЕИЦ_Е  ЛЯСЦТВТИОСЭЖВЙГФВГ_ЙОУВФЕУЭФФОСЧВШХФВФЧТШИУСГГОАТФЖ  ФЫЭОФУСЛЖАБФЕ_ТЕЛТЯЖВЧЧСГТВСЦЦУАВГЮФХВЧСГТЬЖНТЯЖВГФФ  ЛТЖФКСЫЧНЫЧЕЛТДХУУФСБЮТЕНВЧХСГГОАТГЖНТГФЪ_ЕНУЪЕЛТВИСЫ  ЮЕЗАЮРСЯСТГВНДВЫФЖРАФУГТВРСВ_ЕТШБЛФДТСГТВФВЯЯФАТЦОЪЫГБ  ФССТЮТАФК_ТРСЯЪСЛГНЕБТФЕРШЫЕРУЙЛОТУСГЦ_ЦГЪДТРЕПЕЛТИЩЕГГ  ИЛДЧСЯ_ДГВЧЧИЦКЫЦВ_ЧНГЯЧШРНЮЕСФБЖКАЮЕБТАЦЛХРНГЮВДВЭСК  СФБФПЕСЧИЯЧПФДЦВЧТМИТЬЕЛХТУЦТЪЙРУГБЛЙДЕНВЪИСЯДЕЖУБУЛ  Ъ_УРАЮЩВБ_ЦЦЙЪРЦТ_ЕНАГФУАЮЕЫХТЗУУЯЕЕНЦЦПУЭДЕЦШСТУАВ  АЯЕДНЭЕЕТЯЛТАЦИСЮЪШИЮНУСЪСЧЕСЩОВГСИГГЪСЛГ_ПВШХФУАФУС  ЪСЭХАСУИТЬТИЮ_ЕЛТГЛРЫСХУУФКСБ_КСФЪДВ__ЕЫХТЗУУЯЕСТГФПТЯЛ  ВФЧЧАЪФЛЮВДВССЗЮЮСХУАЪНЕШЦЛРТФЕСЖЪБИВМЕФЮДМДУСТИ_РЕ  РШСФХСХФЪУЭЖВХСЗСЦ_ЧТУВЖИЯ_ПВЭБЛТАВШЛТЯЛВФМССТЯОВГЮФХ  В_ИВ_ЪЕЦЙЧУЛЬСУЛТЬЖУУДССХСРСЯЧУЗУАШВБ_ЕФАУЧХХЧУРАЫЕСЗ_Ш  ИТДЭЛЮСОРАХКГТВИСЫЖЕФАЭКГДСУСТЧАИТЯЛВЯ_ЙВЧ_ЗЛДНЧБТИШСФ  МЕЕГЧЕС_ЪЕК_ТСЛТЬФХАБЖБТВШСВ_УГТАЦГХТДВЭ_ШСВТДВЮЧИГССЫС  ДРЕП_ЙЛШСОКТЯОШТЦЖДНСИВД_ТВ_ЧЕСКЪЗЛДНЧБТАЛУЩЦЕНУШКЮА  СФДАБФХАЮЕНИЮТСЛТЯЖВГЧЗБТЩУГЯЧУЛШСРУШВШГТДЕЫХТЗУУЯЖВ  ФМССТЯЛФЭ_СЯЭ_ЕЧВТУЩЕЩЧНЫЖЕН_ЪЙВССЧХУЭЕЪЫГЖХОСОВХ_ЕП_  ЧЕТВ_ЗЦЧЪСГГНЕСЗ_ШГТЬЕОЫГЛУУГЩУШСХСТДШУУЮЕБТИОХУЭЕЦБЖ  Й_РСФССИВБЧЦИХ_КГЗСЖВЫАФЖЧТЕЛТФЕФАИОРШЯОЛТВШЛЗ_ИВАУЛЗУ  ЭЕТАИШЛТФЧИЦЦЖВЕСРСЯЧУЗУАШГТХКИТ_ЗЮЭЯФЕШЯУСТАЦСХ_КЛЮС  ФФДТШСЭСКРССОВЭДКГТФЛЬШБРСЯСОРАХКГТРИОСЭЧБТ_ШИИСЙИВТЧЛ</p>

	<p>ЯСЧВЩЧУСРСЖНЕЭОРАЫЕТУЮЬЛЮ_ИРАЫЕТШБИСРСИИГГФЕЛЬЬИРСИСТ  ФЧИЯСФНАЭФХЭЧЕФТТЕЛТЙИГФБОРНЮЕУУЩЩПШЧШФССИЛЧЧСФССДВ  ЭТМЗНЫЕЗШЯБВ_ЕЬУВЕСДСЭГГДЕДШВЛЗУСЛЖАСЧХУЯФЕЫЭЖФОСКОСС  ТИ_РЕПШЯЛИТАЦЛСГУСРСИФШХКГКЯОИТЙЩХЭЬЕИЦ_ЕРУВЭИДСЧИЯНОВ  Э_ТИ_ЦЖРДТЕП_ЧЕСЙЧУЯТЯЛВ_БЖЕЫЭОФОСФФАУЛР_ЕНАЭРЛШСНГЯЧЭ  Г_ЬДВАСТГВНЛВЫФЖРАФУИТЦЦЦ_ЙСТ_ЗЫШВШЕУСИВЭБЛТАВШЛТЯЛВ  ФМССТЯФВССКУЕХФЖАСОВ_ЧЕЙШЭЖОТЯЛФЯ_ШУССУГТАЦИЧВРГЪТУЛС  СЗГКЬОУИМЕРШСИСЬЮЦЬУЭОФОСЧТАЬФМГГИЛШСЬГВВШЕАФЖОАСИСЭ  БЩЖТЯЖЫШЫЕНВЧХСГГОВ_ЕПЫБЕДНЭЕТВЧЦЕУЯЕРШЩЖТ_МТВЯЧМЗЕД  ЧСФЪЛПТРЕЦЦЧЕФЭТНЮХТСВЙГФВССНГ_ЪТГЮВДВЮЬШИВТШЦВ_ГВАА  АХНСТСЫСКОССШСЦЦЖЫ_ЧЙСТФЦИЯЧУЛТУАОЫСОКВРКРНСОВУЭЛНГТУ  ЗВСХИДБФЕЫИЕФЕЮЖУАЬФЕТЯЛФЭ_СЯЭ_ЕОШГЕТАВСИТ_ЭИ_НЕЛЗСХСЗФ  ЖОСЭЕСЧЯЖЙЧМЕЦЧТССГНЕП_ЧЕРУАОФУГБВБЧЧИ_ЫЦВЭ_ШСВ_ПВФМСВ  ССКСХ_СИ_СОКХЧЧХ_ЕЬД_ЕФАИОРЫГЛОЫСОРАХКГТАФЗТФОЗАЮЕХВЧЗ  СХТУЛСССЧСХЧШСХСОБЕГЕДЮТЙСГЬСС_ЯФЖАСЧОЕЙЖХШЭДВЫГЖНТАЛУ  ШАОФУФЕПАПЕТШВЛРЭДЕБТАФРШВЕИШСРВКФЖДВЬУЦТЬФХАБАМТ_КЛ  _СИСТФЧИЬСРУШАФФДЬЕПАХЕСИЧУЛДНЕТВ_ОКХЧКИ_ЬДВГГОШАГИСВЗ  ЖВБ_ЧОШСТГЮЧУЯЭ_ЙСТАЦИЧЬЧОАФОБТФАРЕЭЕБТЪНВЭТЦПУЯЖВГФФ  АТГЛХВТКНЕСОВББФЬШЭЕИЯДЕФЮЧКЦРКОИТВШЛКЬО</p>
13.	<p>ФЬФЮИЭПЬБДЕКУКШХФРВХФДЙЫЛСМШОДФРЕСХОЕУЦЦТТПЭБЦЕКОДФР  ЕФХШОСЗЦЕЬЩЦЕЦХКТТХИЕЦЛРСЕТЩЧАЖЙЕРМСЖРЖШЖДСЫФЗЗЭОДЙ  КУКОШЖПХЧФОЖОФХФУЬКЖУЕЬЪНЧЙЩИЕТКЗУТЖЮШДКЧРЗМФЦЩЖЕ  ФМЫЛЙХКТТХИЕЦЩЦДРЖЬЖЗМЦБНЮКЧУЖЬИКЮХФВЖНЕХЪХЖЪЖХШУ  ЖЭФДИРЦКНШФДЧЛНЗПНЖРЖЪЛХМНДМПКРУЩЩЦ_УУЕИЧЮКАЖУЕФТРЭ  УЖМАРПКЩДУРУГЖЫШГФЮШ_ЖЧЖРХКХУУЛСШЖЧАЦТУЕСХУЕФЧЩЦЦФ  УСНШЖЕГЖНЧФХЧУНТКЧЗХФЕФХРКНФЩРДПККУКЛКЕТЬДДЮЭФДИЕСДЧ  ЛУКФКИДГЭЩДУУУШЩЮЕЦСЫАФФЮСЕЖПИКЧЖЕЫЩЦЕПЗХФЗЖЬЦУПТ  УКШКХУЯРХЧЬКЙУТЦЧДХЭЕПХЭФХХОФДЕКНЕЩЫЛФМЭЖРЖНЧКЖНЕУЛ  ШФСЖЬФРХСЛТПУЕУЩНЛЬЗЦЕЦЗНЛРВУЭДШЩЕЗОПФЪХЧЕЗШРЕЖМТЕФЗ  ЧДЧПКИУЩКЦЛМКХГЩЕЛДШЮШППКДДЬЩШКТКФЖХЫФЧПЭБЦЕКУУЖШ  ЛДУЩЙДКПЛДЕКРЧХКНЙМЬБДШХЖМЗЦЕГЖЬЕШШУСНМЧЕСЗЫБГЖУИЕФ  ЩИТЗКХУЛЩЮРЗКРДУЩЛОЖХЦУЙЛШНЖУЕТЗХСУФУСЕШЖЕПХКТТМКЭЧ  ХКРЕСКИ_ЖЬЛЖЕКЭШЙЬШЗЪРШКЖЪРЕОЛСЕЖЩУЕЖЬСЕЙЛЕЖХОЩДХЭИК  ЮЛСДЕКЧРЗМАСЖОФРХЬФСЖЗШУЖНАДУЛЦАЕКОЗЗШФЗФЛЕЦСЛМНЩРЕС</p>



ФРЕГЖШЛДЙКЧНТЛЫДИЕСДЦЫФЙХЦМЕЩЖЕНЖТЖСХЦЭЕТКЧЕЙРСАПБЕЕ  
ЫШЩРЖЫЖЙХЬШАЖУНУИЫЖМПЦЖЦВКУЕЖРЙУЖЦОЫМКФФХЧУНТЬДДХ  
ЪФСФУСЦЕКХУЙЭФХЕЦЕУФКЧРЗНЖДЩРЗКЖНСЕЛЕРУЖШЩДИЛШВЯХЖД  
ЦРШХЖЛУЙЧРОЬЖШЖФЪОЖРЖЭАДУРУГЖЦЛИСЩЕРПКХГЩЕЛДШЮШПП  
КТЕЧЖДДПНЖТХНУЕЖЪЛХМЫИЕТЛЕККЩЕХМББДФРЕИХНФХПКЧДФУТДУ  
ШФИХКЧЕЙРСАПБЕЦСЛНЕТЛЕУФЛЕУФКЛЮМКЧРЗМЕУФЛЕЗБВСЕЖУЕЧП\_  
ФТВХФДЦЫОЧЙЩЦНТЛЕЙЙРЦАЖЧАЦТУЕСХУЕЗХЦУУЙЛСНШЖЕНЩЛРДЕК  
З\_ТКИДЛЩТКЖХФСМШКЕФЭЖДУЛЦАЕКОЗЗШФЗФЛЕЗЬЩКНТЛЕПХКТТМКД  
ДЫЩШКТКЧЙМЦЖЧВКЧЕЙРСАПЫЩДФРРУЩЦЦ\_МКИУЦЫФЦБКУУЖЬШЕЧУ  
РДОЛТУЩЛСДКЩСУЙЩГДПКНЕЩХУШТКЧКИРЕШЯУЕГЖЬЕЙХЬЖЙХИЕМЗ  
ХЦ\_ТКЙРЗТЖДПКИЦСЩЦКЖТЖЖБЦГЖЬУУУКХХХЬУШЙВОЦВКХУЛЩНЗЗ  
ЦЕГЖЬЖЗМЦБНЮЛЕНЖНТКШЭФДМОФДЬНОЙМЦЕФМЫЛЙЖЬФЖХИЕСЗЫБ  
ВЖУИЕФЦИТЬКЖТКРСАШХООЖОФРХЬЕКМКТКФЙЕФЧУИКЩЬШЗХНЖРЖ  
ШЛДУЩЙШЖНАХЗТОЧВКЧРЗПФЦЩШФИХКЭШЙЫШЗЗКФЗТЛККЙВЛИХКТТ  
ХИЕЗЖЗШШЖЧОТЬЭЩДЕКЧЪЙЛШНТКЛКЖЫЩПЪКОДЦЫОРВШЩРЖХЕТМ  
ФЕУИЦОЗЗЙЕЦТРНЕУУЕШУУСКФУДДУЛЮЕЖШЛДХЭЦ\_ЙЛСЕЖРЛДПКИЙЧ  
ЮЙДМРЕИЪМРНЖХФЦФЮСНШЖЕСХРПД\_РРНЖУЕГЖЪФЬНЧЧЙЩИЕТКОЪ  
ЖСЖХСУПДПКЧЗМСООЖЪФЫМЦЩОЖЩЙУФЖЕФЧЩЗКНЛСДЦЩЕСФРЕСП  
ЦЖГЖПФЖЧЛДДУЛЦАЕКОЗЗШФЗФЛЕЦСЛНЕТКДДМФЕЖЪПБДУЩЛВЖСЛТХ  
ИЕЦХОСЕШУЧАЖШЖДУЩЛДШБЖЦЩУЛДХШЖДХЪФСФУСЕШЖЕХЗПОДИ  
ЩЙЕЖЮЧФХХФОЦРЧАЖЬРЕОЛСЕЖЩУЕЖЩШТЕНЕШЖЧЛТЕКЧЗХИЕХЪХЩ  
ДЙЕЕК\_РЕЗЖЩХЕШШФЦЩУЕХЗШЖДУЩМКЩКФЧСЫАЧВЬДДЦЩЗКЧРЙНЩ  
РЕЦММДДЫЩШАЖПСГЖЧЛТЕКЧДГЭОСЖЬСУЙЩТДХШЖДЬВСЕЖЩЧЧЗНДД  
УРУГЖНЕШЩЦЛТПУЕЗХЬШУЧОЖДШБЖЦЩУЛДЙЩЧПЧРЧНТЩЕСМШДДХ  
ШЖДИЮККЩКТУЕКФТЗКТКФЙЕРДМОЧЖЗШЕЖЧАЦТЖЕТЗЪФРФЙСЕЖНЧК  
ЖЧФКЖЬЩЮМЬШЗХНЖТПРЕЦЖЭФОЖЪФХБКТТМКЭЕШКФЧЖБЖЦЪКЧЗШ  
ФЗПЦФЦВКСШЮВЛДУРУГЖЦЛЬПЦЕФХЦРУЙЩПДЭУЦВТЖУНСКОЖХКИДС  
ЫЛФХЬШНЖПЦШКЩЙУЖЦЛПЗЫДДФРЕЖБЦФДПКЧРЗНЖДИЩЙШЖШЛДЪЧ  
УНЮЛСДУЩСУЛЩЧВКОДЦЫОХХПЖДЬЪРУЧУСНЖЧФКЖНАМЛЩЦУЙЦЛТ  
ПРЕЗШРЕЦМЧЛОШЭИУЖХФСМШКЕФЭЖДОЛЕСФЩГДЪ\_ЖЛПНЖРХКТЕЧЖД  
ДПНЖТХНУЕЖЩЩДУРУГЖШЛДХЭЫУЛУСЕЖЫЖМЪЧЛКЩЪДДЦЫОДЦРЦЗХ  
ЧЕШЛЩЗТХЧЕЦТЮЭЕМКДДЦЫОТЕЦГЖТЖДЦЫЛХЙЛУТХРЕУИДДЦФРУНМ  
КОДУЛЦАЕКОЗЗШФЗФЛЕЗЬБСШЯЛСЕЖЧЛТЕКШКЧЪЛРПНЛКЖЩУЕЖМЛМХ  
КИЦЕХФИХКМКУЛУЦЩНЖДЦЫОМФЛСЕШЖЕСФРЕЗЖЬЛХЛРЭТХФЕЦСЦФТ

	<p>ФЩЧЧПКОДШХЖМЗЦЖДЮЭФДМРЕХХПОЧМЦОДСЩУКЮШФДЧЛК_ЖМЩЙ          ЪЭЕКМКЧЪЗЫШНДКУУЖЪФЙЪЧЖОЖ_ФХХВЛТВХФДЦЫОЖЗНОРЗКФТЗКЧУ          ЖЬШУЧЩУ_ЖЭИУП_ЕХХПУ_ЬКУКЖМЩЙМЭЕРПКХХМЪДЧШЭИНЕ</p>
14.	<p>ЦЕТЙЖЗКЦОНКФФЗРРЛУТГЕННЕУДХШНСУЪЕТЛЦЕХЛЦХШЬЧОРКГЕЗЕЭЛРК          ЗТКЪЧЛДЬУЕЭНЕЗХУТАСКХЖЦЬШМЙЛГЕУКЧФСЬШУКСАДЬРАЭЛРОДХЕР          ДЭ_ЕЙЮСЖКВАЕЪРСЕБЭУЕПЩТЭНЭЦДДЬФЦУЪНСДЙДЛИЩДЗУОДНТЛКШД          ЩЧИКБЕСДЩТЕФЩЦТУЭХОСКЗЖЛШУЙУКФФЛСЛЦЭДЛЮРДУНБКЙУКТЛД          ННМШККЧРУДМККЧЩЧКУУДТЕКШЧЕСЦЙДОДНДЦЕЬЦЛГШНОДЬЧЖРКТЖЦ          ННЧЧЕЗЖЧЖДЪХЛТЬШТЦРШИДЖХУВЕТРЦТУЭХДДШЕЕЗЬКЕТЛЭОДЪХЛЙЩ          ЦШУЫУМТЦЦШНКЗЛЦЭАЕУКФФГНРЛУТГЕННЕФЮИЖЪРЗЖДЫЕНТРЦСЕЪАЕФ          ЩДРХРФФЦЭНЕННЕУДХШНСУЪЕЪЩЧБДУДФЪРТЪДЮЗЖЛЛРЕЦНУГДЬШХХ          ЮИЩДШУЕТУДНЕКЪШУКТЖДЪЗЛЧРДУККУШПЫ_СДМ_ЕКФДШЕФТАДНЗЛХ          РТУУФДЛСЮДХУКЦСШСЖЛДЬУСШЬНИДЪНЧАЧУЕУЭДЙКШКЦЕЦЕЕУШДК          УНУСАШУЕНЬПЩЦШ_ТДЩЖЦЕТУТДН_ХХЦЗФЙУРЕЗЛЦОРУЦЩДРИФХЩЗУ          ШКЦРЕТЕИДРОЕЖЮЙШУКЖАДЩЧЛЫКИЛХЛЦОСКФРЮЬОРКННДЩХЛТМ          ШЦИЛДРЕХНЛДЭУЕЬЮЙУ_РДОМНКЧЧУГЕПЩЧФХЕКЕЦЩЙЛХСНШДНДИКЦ          НРУФДШЕФТЛДНЕЧНЦНЧЕККЙУЫУИТЛДШУЭЪЖЦКМЖЪЩЧЛРЛДФЧЪХЖЗ          УЧБЦЙДИДОУЧЧУДРДЪУХЕПАЛДУДХУКЦФЗРЧЩДУЗЖТЛДРШТСОБЛДИМЙ          РЖДЪДЧУМУГДУДТЕВШЕЪЭУЗДРОЕТРДЗ_ЦУЕЦХШЭТЩДФЙШУПДУЗЖТКП          ЩМЧНЭДЩЩШЕНЭОЦЖДХУЦТАСКЪФМЙНУУЧДШУЭЪЖЦКФФЦЦЕСДТЕЕТЛ          СОДЛДХЕЦЕЮПОДНЕЪКЦДНДЭЩЦЕУДБЧФЖКУУЕКТЛДЧУЙРЛДУЕБДХУП          ЦСШВЕШАКЗЖЦУРОЦЛДЛИЩХФЗШЕЕЗЦМИХЛЧОРЛЦБДПУТУФДУККШЧФ          РЗЕТУЪЛИЩДИ_НККЕЭАЕУЭДХУЪЕКАУДОДЮМУЕЦЕЕЪЭУЕЗЩДИХРСДДРК          ЕУЭЦЩЧЪЧИНЙДЗ_ЦУЕШКНИЕШЕЕПЮМТНБЕЕЦЦЗЛЮЛТОККНЕЪЭУЕФЛР          ЖЭХЕЕЖЕРЖДЪУКДТЕТПЩСЕУШЕЕЙЩИЖЙЛРЖЦЖДЭЧЩДЗ_ЦЕЕУМСЖТЮ          ЧЖДЧШМКЧДОДЪХОЦЭШХНЦЕЕПКТЛСЮДЧДПУХХЦЦФСКТФДУЗЖТКПЩ          МЧНЭДЪХОИЩЧФЗУРЧГКПЕТЛФЖЙРТОВКУУДШНТЕЦУЕТРДЧСЮЧОРЬГЕН          КЖФЙЫУЕУЭЗЛЪЛРЕЦНУЛОКРГЖЦФАЧШУПДЬУМНЭКСАШНЬККЕЕЦЦ_ЮА          КЧАДЧЕШШВПЖДМЕЗ_КТЖЭУДИМПШТЕЦНЕФРЬОДЭУХНЭАЕЦЩРФСЦВЕЕ          КПЖПКУШДЭУЙУКСФЛРЧЕФЫУОМЦОШНКТЛЦБЕЧЧУКЕЧЩДДДУДФЧПЕС          ДЬЧЦУОНПДЪХОПЛМЕЗЪХЛЙЖДЧУЦУТУИДЗЕМЕТДЪКЭКФДУККЧФФУЧБД          ЛДШУЪНШАКЪИУЫУЧЧЩСЕНКЗЖРРЛУНХУТДЛДКРЙДЭКОУЕЛКЖАРЩДШ          КМКЕМЛФОХЛЧБДЪЕСЕВЩДЬФЦУЪНСЕКПФСРТКЕШЧЮЕКМЖДБЧФДМКК          ТЛГЕЙРЗРЕКФЦУЪНККЦЕЕЗКЪЩРЛТЛДЬУРЕКСАДШКЕЗЩХФЧУРОЦЖДОЗЛТ</p>

	<p>ЕПМОТНБДУККЖАРКФЦНОУШУНРЛТКПЕЧЛПФЗЩСЩДНУХХЩЩЩДЩТЕМ  ЛФЩЧЛРЧГКНЕФЫУЗУЫСФЧЛРЕЬЭУЕЧЩДФЬРТЬДШКЧПЩЕКЩКЕЗЛЦОРУ  ЦЖДРИФХЩЗУЕКШИНПКСЕКПФЗЛХЧЧНУЕЦНУЛИЩДТШСЕЕТЩДНТЛГЕЬЭ  УЕТУЬЛИЩДФЧКТЛИЩДУККЙФЖЖКШЩЙДХХРПЩЕЭНСЕКЦИУУДИУЬХФЦ  ЕДОДТЕИКЦЕЕХРЬБЩДЧУЦКУ_ДФИЮХЬЕ_ДРУЭУЦ_РДЖПНОРОТЛДХЕЧЩ  ОРЩЗУЕКФЦНОУШУНРДРЛДЧУНКЦЭРТУУКУЧУМКУТЕСЕУМХЖМЩСЕЗЩД  ИЦИДУУБАЕЗЛЦОРУЦЖДРИФХЩЗУЕКТЛДЧУЙРЛДНЕЬТЩЧЖДОДШНРЕХДУ  ККСФИЦЕЕЙЩИЖЙЛЧЬЦЙДЭЧЩДЗ_КЧЖПЩКЕЖЕРФДНДЙУЦУИКККЛДЧШ  МЕКУЕЬРСЕЖЕДЛОКТЛРЖМДМ_СУКМУЕЭАЕТЛДКХЮИФОКЙЛТЖДИУТЗЦ  ЕГЕДЦЖДФЧКУЗКПТОДЩТЖДЮЗОЙРРЖДУЗЖТЛДОИШЕШАУЬЖДХУШУЫ_  ПДН_ШЕЬПОЗЛРЕНТДХШВПОДЭХДФУЬРНКПЖСЮЭРНКЮЛФХНЕЖЛЖРНКН  ЕЦЩХЕЗЫГРУОУЕХЩЙЖДТЕХН_ЕУТЕОЕЗКТЛККХЛЖЙЧОЭХЕТНКЬШУКЖАД  ТТЖЬУРОДЗЧОДНУЛТШ_ЛДЪХОИЩЧФЗЦКУНЙДКШЧЕСЕКПФСРТКЕШЧЮЕК  ШМДШКЕЛПШШДЦНЕТЛФЖЙРТОГКУШДХНЦИУМЬКНДУУКТЛШСЧФДУЗЖ  ТКПЩМЧНЭДЬЧЖРКЖАДЩЧЕСРТДДЭЕОЧЖДШЕХНЛДЪШЧЧЙПОДЩТЖДХР  ОПШШСЕКНИЕШЕЕНОТЖЧЖНЭЕКЦЕЧНКЦЙЕСЕТЛСЛХРТОКЧДИ_НККЕЭАЕ  УЭДУКОУЕЧЛОУШКПФЧЩХЖГКСЦЬУРЖДРКЕЙЛСЧПЩКЕРИЖФФЕЧЧЧНУЕ  ЗЛЦОРУЦЖДРИФХЩЗУЕКЦККЦЕСЕККТШКТЛЦХУСАХУЕМЛСЛЬЛТООКПЖЦ  ЛЧЛРЖТФД_УНГФЦЩЗЛДРЕХДЧШПНДДШЕЭНШЕГЮУОЕЦЦККЦЭЗОККЗФФ  ЫУЧЕЧНЕФЩЩШУЫУУТУСОДПЕЗ_КЦХКЫЗЖДЮЦАФУЧЬДЩЩШУЫУМТЩЦ  ШАКУШЗРЧЭНХЕЕФЩЧФСКФСЦРЭЕНДУКЫПФРЖПФДЧНУШЭДФТЛДЙРЮ  ЖФЩЦДИМПУЫТЮРЖДУДФЛМЖРЛДРЕБЕДДОУСУНУГДОУЧФЩЙОДМУМ  ККСФОКЗОЭЖДРЕХНЛДШУИУЬЧОДБЧФДУМЕБЭУЙУКЖЩЙРЧ</p>
15.	<p>ШШВСОЗСЯЕНФЯЖЧМЪЭДШТТКВЪСДЗГФД_БФИЯФФХЩЭЧГРЬЕМСЫЩЩЦ  ЭЕГШМРДЮ_ЕШЧЧЕЖЛЭФД_НЙЮ_ЕЗСВОРЩВЖДЦХФХЯФУЕРАЦНЮДКНЬ  ТЕКФ_ЕЗЯСИЦЦЮЕФАЪНТСГБЦПСКЕУСЛСГСЧРЯФФДЮЧЕХСВЧПСЩАЗСГБ  ДЯСШУЭСУНЫ_ТШРФЖЩЦЭОЦССЛИЯБФЗЮТЕЦХЧЦЛСЭЖДЬФФКР_ЗКЙТУ  НЦСОДЮЪРУЭДЕТЦСЧПСЦЖРССУНР_КТЯХФДБЭФЗССРХЯЮЛДЫТРД_ХЕХ  НЛДЩСШУРАФЧЯЮЩДВ_САЫ_ЕЬВ_ЕПЯБФЗССЛКРЖФЙЩЭЖДЦКЛДУСЧЦ  АОДЩСТУФЭЖДТМШАРЩЖЬУТЭКЮТЕМЪ_ККПЮОДУВРУАЧЕЗБЧЕМСХФЗЯ  БОРЩСФД_ДЙЕЗЧИКРГФРЫЪЕЖЛЭОДАТНРЦИУ_РЬФСЦЯКЕЮГЕФЯВСЕЬСЦ  ХПЦУНЫТЕЦРАФХГИЛТЩЧТДАТНЗЦЦЖЧМСЫУА_ЮКЮНРУР_ЗУРФЧКЭСХУ  РВФЦЦУНЭСЧКЬЧУНПЮЕНРЬЦК_ЧЧПЮЕШАРКТЩЬЕЗЯЩИХСГОРБРЕЬЦБ  ЛМРЦИЕРЦУГРЬЕУТЛДЗЩЭЕЬВ_ЕЗРВШК_БЕЗЦБЧРЩЖДИЧЧМЦЛЦПГЕУВ</p>

СРХЦАФЦВЪЕЗЩЦЛРР\_УДЭЯФЛЦВШЗЯСФИЮЧПДЩСЧРЛЙЖРР\_ШДТТЮПЩ  
БЬКУСЭЧЯСОЙЦГЕТЦФЛЙЯЮЖГРВОРССИФА\_ЭКЭСУКРЮФИР\_УДБЪЖМСГБ  
ДЮБЭКФ\_ЕФЯЭФЛЩГЛРМЯФИЯСХУВ\_ТШРИШУРЧЫЕВНЕЙСЭБЭЦСХУТ\_ДР  
БРЕЗРЬЦК\_ЧЧЩСТКЧЩДЫТНЕЫТТНРЩЖСЦГУУРВШЕЬ\_ЕТЦ\_З\_ЫЯФЗЦЯУ  
УЦСИУЪЯЛТЩЧЕЗЯСИЦЩЖЕШЬЪЕЕСФТЩСШУЪАОРЩВБДУСРШЗЬОДВЪЫ  
УРБЖМФ\_ИЕАЪИЕЪЪЕСЦШКШРВФЖЯПЕНРБЖЦЕ\_КНЬЪЧАРДИНХРЕЙАТЙШ  
ЮТЕНЬЪЕИСБУНШ\_УТЯХФДБ\_СЙСГЖД\_ЧРСЯАДТМСНРЪЕТЩЮЕРСЩЦЗ  
ЪРНРПСЕЪСРХЦКЛТЛЫЕПСЭТ\_ЫСЧЙЦЭЖРРЪФСЦЯКЕЮГЩДУТМТЯЧЕЙЯЛ  
ЦЦЯОКРАФПСЩЖТЩРЕШАРКТЩЬЖД\_ЕЦЬ\_ИЕЭСГРСРЕЖЛЭОДЬ\_МТЛСХУР  
ФФМУБЖЮЦЯОНРВИУЦЮЕРГЪЖЗЛЫЕПСЩЖПР\_ЗЯПФОРРВИУЦЮЕЧЯФЖХ  
ЩКЖСРИШУР\_УДТМСДГСЗШЮГФЗЙЪРУУСХХЦЦЧСФСГВВДБТТУЭДЕНЕ  
СХХЦЦИУХЪШКЪПЕПЯГФХЛЫЕЙЯАЩЦВЪСДЦХФДЫСЧЗЯЧПДАДРКРЪЕЙЯЭ  
ЙУРВЕТЩЮЕХСЩЙУУТЦНУТСДЫ\_ТКЮЦЖТВСУКЭЧКРЦЯУУРАФЦСЦОРРД  
ЦГХЯОПССХУХСРЕАТЩРРТЕВЪТДДЮТНТСИОРРЯЖДЦХФДЭЧЧЧЯСВЧССУУ  
У\_ЧЧМСХХЩЯДЧССЗ\_ЪТЕПСЩЖПСЮОДБСДЗЮМТДЮЧЩЙЯФФРМВШЗЩЧТ  
ДЯЯОДФБФСЫ\_ЕХЯАШЕЪЪЕНРЪИЕЮСОИЮТШАЩИЕНБАФРЮЪШКЪНЕПЯЮ  
ЛТХТУЧБЪФИЯСЦЕБАФХПШЛТЩРЕЦЪМЮЕБСЧЗЯЪТНРДЮЕЭЪЕПСЪЕУЮЪЕ  
ИЯФФХЩЭОДУ\_ШДГШФДВЧЗКРУЩЙЦГЕИСБУНШ\_УТСРЕПАМЧЕРЬФСЦЯКЕ  
ЮГЕЙГЮЖРРФЕЧЯГЕЛЦСККЮНЕЙЯАЦУБЪШАРВИУЦХФДСБЛЦВТУЧССУУР  
ДЦГХЯОПРУЛЛСЭЕНШСХУХСРЕАТЩРССИКА\_ДЧЮ\_ЕФАЪЕФЯЮФЮЩСЧЗЯ  
ЪЫДЦЦОТЯЮАЭЪЧУТЩЬФЗРЯФЗЯЧЕУТВШУПГЛРМВШЗЯСЩЦЦЭОРЯСЗКБА  
ФПЯЫЧЧУ\_ЕПЯЮЛТХТУЧССЧЪУТЭКЮСЗ\_ЪСЗЕИЪОХЦЗЕЦРФФМЭДШНВЧСА  
ЮМТНРЭОЦВТТНРАФДБЧТШРВСШЗТГДЫ\_ТКЮЦЖТВСКШЭТСДЯАДЧМСЧУ  
ТБЖЧМСЧЗЯЪЫДЯЕОЫЩБФЗРЪЕЙЪРЕЧЯХФДЕ\_ШКЪСФФПГБДГЦЖРЩГБДУТ  
ЧНЬЪЧШРЧЙУА\_ИТГСХУХСЗРСХФЗЩЦУ\_ЭСХХЦЦСУФ\_ТДЮ\_ЕПСЪЕНУТУД  
ЫДНСЩИЕЖЛЭЕЫЦЭФЗЦЪЕЦСЮАОРАЦГЭ\_КШИЯАОРЪЕФАТИЙЩФАОРГФД  
ЩСУКРЯЖЭЦЭЕЙАДЙУФ\_ЕЦ\_ЧУТТЕПА\_ТКРЪЖПРЧКНЮ\_МЙЛСЩЦЦСОСРД  
ХУВБЛЖЪЧУТЯХФДБЭАЭМСШ\_РФЖЦЦЭОЦССЛИЯБФЗЮТЕЦЫТНЕЪСФТРЧП  
Д\_РЕИЭОЗСРЕУВЧЪДФЧЦЕБЪТД\_СШЗЪСДФ\_ИУАРШДЩЩЕИЯБФЙССХУЪЯ  
ФДУБЖЧМСОЗСЯЕПГЩТНЗСХКАЧЦЗСЭЖДЫ\_ТКЮЦЖТВЙЖДВЕМЮТШАР  
ЖФЫЦЙБДБ\_ЗХСГБДБ\_ИКЙТУНЦСКЕРУЛМРЮЛТПСХУВ\_СПЯФЖЧМСФЖРЧТ  
КЪНДТЦСХШФТЭКУЧЕЙССНЕСУКРАЦУУЧККИНЕНУТУДЫДНСЩИЕЗЛГЖХ  
СКОРРХСЕШТЕТГСТЕВДЮПССЧПСЩЖРР\_УДЫ\_СНРГАДГШЛДУВЛДШЯЖКИ  
НЕЧСЪЕФЯШЖРГЫЕУБГЖЗСЫЧГРЮАД\_ШУЪЫЩКЭСОД\_БОДВЧЗКРГФДВ\_Е

	ЖСГБПЯСТУЪСФЧУЧЭЕЪТЕУЮТЕТЦСШКТЧЕЖЛСЫНВБОЧМСХУБМСЕЪСРЕР ЩЖДЯЕОЫЩБЖСЩ
16.	КФХ_ПГБИЭОЮ_КВЬОЩНТЕЗУХДТСПРНЗЪОЗЖФЕЗФЫЫ_ЛБСЖВТИПЖПКЦ ОХСЗТЮ_ПЛЬННМПУУЛЕЕЗЕПОТРРХЗСУННМПУОИПННХПИЗЧЮНИУШ_ЧС БУЭОШ_ЦХПЦНУЪВНМПРИКЭОЩББСЖВЧВЫНШ_ТСЫОТСЫОКВШ_ТСЫЫЭ ГОСГВЭАМВАПЖЬШМЗЖЮРЦЗЮМЗТЮМРРРЮЪВЮБЗЦБРНВЭАЗЦЫИЮГД_ ЧЦАТЦВ_ЕМНЮ_ЛЗХ_ЧУЮМНФШТЗЦЧКРПШ_ЧСЫОПЯОМРВЯЕЩСЪ_ЩЦВАН НЖЮМЗРЮЧХСЩ_РКТОПЪШКЗЛПНУХБШГТШРФЛ_ХГПДШЦУОСВВГЦОПЗ ИФЭЕЪВФОЛФАЖФЛ_ЩИФОТГППШСЩДНХПСЪГ_У_НР_КВЕЕШНЮВГВУД НВВЖЗСБРИЙРЯЦЯПНИВЧОУСБЫЭВЮКУГФАЭВЪРИФЭОЗЛПРНЗЪОЗЖЮРЖ ХПННФШМФИБРРЪЭОЗУРСЦХРВУИЭНВИПВЦФЪОКЮХ_ЩЕХЧРВ_АЙСЖИС ВЭАШСФ_ЫЙППЦЗЭИФГХТЩБППЦФЫЕЗЗЮЛЛСЦ_ПЛЬННМПНЦЪШ_РВЩД НХПНИВ_АЙСБЫЗГПУЗЖЮСЧСФ_НЪХ_КИЖЕШВТ_ЦЗЭОФВШЗЗСЪОХВЗЕКГ ЫНВШЗЗТЮДЗКРТКС_ЕХРЮЙЗФБАКРШ_ЧУЮТРЕВЗИНЮНХСПСКИБИЪФО_ ЦЖЮНГВВ_ЧСФЪНКФАЗФБОЖХПКИУХТИВААХЛПИЗЛЧВЦКЖИТЛПСЪИАНР ЕЗИЦЯПЗИЗЪАФЛППЦЪБОКГО_ЪУЮЙТГПСЪСШТЗХВТЗЙХ_МЕЮРХЛЬ_ПГЪ УЪГТШРФЛ_РВАЪНЙШВ_ЛАЪЗХЮЧХСППШБЖЕЪФО_ПГПУЛСЫ_МСЪАЗЛПЧ НЖЮ_ЧИ_ЕУЛТАЕХПИПВЯУЩХЮГЦВТ_ЧС_ООРХЕЗЗВМИИБ_УГЪЕСВА_ЦФ ВНЬЕЗИФФО_УЛЕОФВАИМБПВЗТХРНЗЭСВШ_КФХ_ХГПМЦИПДНЙВРЦХТ ОЗЛЧ_ЩСАЕМРХЙЗФТЕЪОЮЙЗНИОМХГБКРВАЛВЫРТЩБПГЦОЮСИВБРНШП УОЛЭАЕЫШХЗПЮЛЦЗКХЗОНДНМПОХЛПСРЗОТЗЕПКЦПЭАЪИПОТСЫЮЗФБО УГПНИВЪОЪС_ОФВАТЦББ_ЦФБАЪНШ_ЫЙШНИВШ_КЛЭАЗСФИХВЪАУИЭЪТ ЛЩ_ЯЛАТНРЛКРМПХЫЗИЮЙЗЛПДЫУЭОСВАИМЛЬ_РВАМЦХ_ИЪВЭАЗСБЪНК ЦАЕЪХГЦВФОЙУКМРВВСЪГЫЫФЛПГУГЧАФЛПДШЦУОСВТЫЩСЪИСВЫЕОЛ Б_ЧСФЛНВВСЪГТЛНРЭОЛСППЫФБЫФЛПБЫХКЛТГЫИЗФБОУГПИЗЛУРИИБ_Т ОНЧРНЮМЗЪРСЦЕПТШИБИСВТ_ХСТЕХЯЪОФВЯОУЦЗУЙНХ_ЭСФИЪВЯОЗН ЮМХГБЕЗЛПИПУХДТГПОЩХРНИЕЫИКГОСГВИЕУНРЕЪВЫХЗРЛГВТ_МСТО УЯЭОЗХЮЛЩХКХЗЛПСРОЛНВШПНЦВА_ЦХЖИАИЭНВПШ_ХСУТЖПШ_ЧГЫЪ ЮГД_РВТСНВЖЕФЦПТЦВВЛВДРЕЪФО_ЛОРЗИВШ_УЛЕОЗИУОЗЖЮРЖХПОХ ВУОКС_ИЪВА_ОГ_ОФВШ_ЩВЦЕЩХРМРВЯОЗЕШДХСПЧЪСПОХВЭЗРРХЦЗ ШТЗФЫОКВШ_КФХ_ЩОЮОВИВЪОЪС_ЫНВХМЫВЯРРШЮДЖХПКИЙВТЩБПН НЗЮСЪГБОЯРКМРВЖТЦДК_КЮ_АПЛЬЗЕАЕЗЪБОЗТЮДЦХВПРОЮ_НПВ_ТВ АЕШЗЕУЗСЭ_ЙИАПШИАТИРЭОЗЦЫЫЙГХТЩБПТНТХРГВЪООРЮ_КФХ_ЩНРЗ ИХЛ_ЛСТОШЛЬ_ЦХЙЕПЙРЮАЛЩ_ЖВЭЕЗХЮ_ЯХЮ_ЦТ_АКЗКВИААЪЗРЮ_ФР

	<p>Х_ЙЮПХЦХХЛЦФЛ_ЯХЮБВВБЫЗТЮ_ТУРЙХИЩ_ФИ_ЕЗТЮНЖОПМНРО_ТГЪ  _ЖВАЕЙБППЦРШМИАПАЗРХ_ЪГЪ_ТГЪ_ЧСЗЛЦФБЪЗФЬОЪУШТЗРР_ДХЮ_МИ  ЫОЗХК_ЛСТОШЛЗЪЗЪБОЗЫПВРРЮВИХППНУХДЗРХЙЗССРИЬРЕЪФО_ЦРПКЗХ  ЮМЫВЪОЪС_ЫСВФОЙУКМРВУЛИКРМРВАМЦХ_ИЪВЭАЗРХГЦВФАЗЕШНЦЕ  РТЗСБВНЪРЕЪВЪАУИЭЪТЛЦ_РВФУШРЮЙЗЛПКИЙХТЩБПЧЪСПЕАИПБЦОЛ  ШНВФОЙУЮТВВЩ_ЫФБАУСАТРВТЫШГЦАНХАЯЗЕПЕЛСПВПЖЫАМИПЯЗК  ЭАЕВЮТЯИУОЗХК_ДХЮ_ЛСТОШЛЗЪЗТ_ОМСЫЖИИБ_ЦХЙЕПЙРЮАЛЦ_ЙЮБ  ЪЗОНБРПКМЗТЮ_ЪЕЮЕФЦПТИНЮЕЗЙХ_ЩЪРСЪЯХ_ТГЪ_УАСИЪЯПИЗЗЮВЦ  ОЛНЦВЭАЗЕАЮЗЙШЗХЯПЕЩОШ_ШГЧ_МСАТРЖПЕЛСПДИВЮЧНРЛ_МСТОУ  ЯЭОЗЗВШИВЪОЖВСОУЯЗЕЗЪХМЗРВЖХСППЦЗБВНУЦДИИБ_ФГЫЕХЯЪИСВШ  _МЦ_НЦМПОЪН_ЫКГО_РВЧАТУКВИБПГУГЧА</p>
17.	<p>М_ЦУЫЕ_ТКДЙЕЪБУРПТУУХЕАНЧ_Х_Х_ЕЕФ_ДЗШБЪЙПНУПККУЧШЛППШ_Х  _МАЯНЙСЦУЛОШТД_ГШЫСЮНП_ХУНАЕ_П_УХОШ_П_ЯВОИУЦШРЪПШВО  ЪЙГЪЙШВУЦЙМБРШДОЪЙЛЩЧЙОДЧКВЛНПСТДЛЕЫДЪОШНЪЕЯКУ_ШРИ_А  КНОУТП_Х_ХОУТТКФПТХУТТ_ЗНСИККЫКЪЪЙНЪДЦОГЕХЪА_Я_БПШВУУЧ_  ЦЦП_УН_ДЙПЛФЧЕ_ЪДЧИККНОУКЦУУТП_АШРНБДЛЫАУЙИУТТЧЕУЙЕЧУ  ЙНЦДЫВТМДВФРШ_ЖДЧЕЧУЙНЦДЛЫАУЙНЪДЫЕ_АТ_АНЙОЕКАЕДЧМАУТ  Т_ЦКЪЫУТТ_АШРДОДШНУТТ_ЦУЙЧЕУЙНЦДМЕГНХ_ЪДЧИККНОУТП_ВХТЗ  АЕМАЯДЧОУТП_ВХТЗАЕМАТДЧИККНОУУЧ_АКЙТЪРЕКБДЧЕУЖДЛУСЪАКТД  МУЦФУКЕЗЩЪСЙИУХПЗБТТРЖВВИ_ДЗНБЭПЙУЕЙНФФЪОЕНМ_ЖЗХЕЮЕХС  ТДЩОДЧШАТШ_БТЙРЩЭТЛУЪБОУРЗБЦНЙНЩЧЙИУЗЫАЮНУ_ГЕС_ВХТСЖ  ЧЫТЦНП_УХОШУУ_ЪДФРФЦТВБОЙЖЩТВИА_ЙЗФЦЪАЦРИЛЬДПГБДСА_НЪ  АЕАЙОАДОАЦТШ_ЫТКЛУЪБОУФШЧЩЦЪИУНЙЗЦЕЧИЩДМЗШУЪ_АУЙЧЖЗ  ЫТЦУМАЯДЧЕЦУХЪАУЙУШУМОЯАЫТЦНП_ЮУНДФДЧАУЖКЛЩДЦОШЪШ  ДЪРЙКУТПМЖДФНТМЕ_ДКЪГЪОЙИУИШВБХТЛУРКСЮУМЫЩДЪЕКНЙНБДШ  ТШЕМАЯЦИ_БТЙВДКЦ_ДЗШИ_ДЭВЯКАЕАНИМУРТШПДЧАДЧШЛППШ_АЕЫ  КБРЕКБДШНЪДЧЕУЦМЯЫ_МАЯНЙЕЧУЙКФПЙТЪРЕКБДШТШЕМШЫЦЕ_БЙЧО  _ШЙСЕХПМЯКЧИСДШНУТКЧЪТКЛУЪЭЯЕАЙПГНЛЛЪЛПНЪКЙТГШОАУНЙББ  ХЕБОДЦЕЯУАНБОЙББХЕБОДЫ_ЪНСНЪВЙОАДТНДЧТНЮЧТВАУЙТЪХШПЪРЫ  ЯУУЪОГЗКТПЦИ_БЧЙЧЖЗЫТЦЕЙИЯНЙДЦРК_ЪДМОДЦЪААУМИЕАЙСЦУЗ_ДЗ  ШБЪЙЭ_ЕЕФ_БТЙНФЪТНФРЙСЦКЪСЮШЗ_ЪНСНПДЫЛЖЛЛУУЪШЗТОЫТЦУЙ  МЖМДКЖДФОЕУЪОЭДШДАУЙВГКЦЯУЙЭМФРЙПЪЦМЯЕНЪУЦПБТДТ_ШЕР  ЕУРЗБЪЗЕ_ЮДРЕАЮТНФСЙВУПШТЪХЭЮУУЧ_АКЙВЩХТЛУУЧ_ГЕСДЖСДВ  ФРЙНФЙТЦСЙКЖЙК_ВУХОЪНЪУЗЫЮУЪУУЦТЛЖДЦОЯУООДЧТ_ЕУХЪ</p>

	<p>ЮУЙРФМЙВУЛТЗАНИБОЗКЮМШЗ_ЦДАЕЯУМЕЮКЙНФДТСЮШЫСЕЗШ_ЯНИ  НФДЧАЖПЭ_ЯНИНФДХЮХУМЬУРТ_ЮДРЕАЮТНЦДТЛЬДЧАУФЪАЮЧТЧЩЦ  ФУСДОЕТЧПЛПТШСЕАЙНЦДЫИЯШЙУ_ЕЙСЦХОЦФДШБГЕСОЦЕЧИТДК_ЕУ  Ь_АКЩОЦЧШРТВВИЭЦИ_ВУЪЫЩДЪУУТК_БЙТНУХКЗУЙКНАШЗ_ККХОЦКФУ  УЗХАДЧЕ_ДЙПЛФЧЕ_БМЙСЩЖИ_ЦЦП_КЧШ_БТЙХБЫПТУНИКФПЙЕ_ШЙКФЛ  ПТДГЙИУНС_ЦЦПГБДЦИГЕЙВДКЙЧЕУЙЕ_ШЙХБЫПТДГЙПГЕМДФДЛЫЦЕЗТУ  РЗДЪДХИЛКЧНОКЙЭУНОУФШПРОЗК_ЮУЪОГ_П_ДХКЗЖДМХБЙИ_ЦДРИЫТЕ_  АЕОЕЦЕЗТУТК_ДКЛЯУФПРЦ_У_ВУЩАЦЭТЙДГЙХБСЭТУНИЧЩЦЪНБДЪАХУЪ  АСЧЙВУТПМУЙШ_ЮУЧЦФДРИЫТТ_АУЙОЯКЧИАДЫЛЬЭФО_ДЫИЯАЧОУЦШ  ЗАЕМАЯДМ_ДКЛЕУФЪИДШЬСЕЗТЕУБЪОЧУЙВДКЦОЧШВЕЧУЙББИК__УХОШ  УЫТЬДЖТЖДЫПЫЦШБАУЫТПДЦРЦЗЪАЕНЬДГЙВУУОНБДРЕЯЕЧИЩДМ_Б  ЙЧУУСДСЯАЙСВУЫОХТШСЕАЙЗФЪШТЩЧЕ_ЪДЫДЦРКТПДЫПЫЦШБАУЫТ  ПДЛРЬЦТТПЦИ_ЧУХОЦУУ_ЦТТЗУЗЙБЩМОАТЭЮУФЪОВЕЫТПДЧЕУМЧАТ  ДСАУЪОУТП_ЫТКЯУМКЧЩСЙОАДЧОДНХ_ЦДЫЕХКЙЭУЙСБМЧААНП_Х_  Х_ЧУЪДУНЦ_ЪДЫА_ДЧЕУМЧАТДЖТБИШ_Х_Х_ДЪКСЕРТВУНЦ_БТЙЛСЖТЛУ  ЙШ_ДНЯ_ВУЪ_ЕУХЪЮУЙСЩЖИ_БЙЧОЧУЙИУТП__УН_АКЙЛСЖТТПДЩОЕУ  ЦУУЪОУЛОАЯДШТУЦПБТДЩДАУНОУЪШРБЭПГБДТ_АКЙУДФЛУКВЕУХК  ЗБЪКРБЗКТПЦИ_ЦДЫА_УЦ_ДКЛЕУШПЗЪЕИ_БМЙМБЦФВОДШНУТКХБЙТЛДГ  ЙВУЧШМУЦААДЧХИЦУЦ__УХОШУЦ_АЕЫТГУПНЬНИДЖЪК_ЮУНДФДЫОЫ  ТКВУФЪЕЪТТЕУУБИХПТ_СТШШФДМДГШН_ДПКЖЩЧЙСЩЖП_КЧШ_ЦЦП_Р  ЧШ_Х_ХОУТП_ЕУЙЧЕУЙВДКЙПГКРНЦКЙБОРШ_ДРЭЧФОЧОУНИНЩМЧАКН  БЕЯАЧОУЪОУУЧ_ВХПЖШКЙНЦДЯОЕКХ_ЪНЪУЪШРБЭПНППШ_АУЙЧЕУЙ  ТЦФПРПДЫ_Ц_ПЗШУЦ_ЩИШ_БМЙМБЦФВОДЧАКНЧАЩЧЫЯУТШВФГЙЖЪМ  ЧЪУЗЙКБЧШРБОЙУЪКЙНЦДЛУШКЪ_ХУХЪЛКЙТЦЪЙОЛНЛОЮДЧЕУЖЭДЩЦ  ЙРФЦФАТТТЯУЕЙНФЗПРАУП_ХШОЕЕДШДАУЙСКЕЫТЬК</p>
18.	<p>АУ_ДООЯАБУУШПХЪЕХНБРПЫТЬЕД_УАЧЪОУХШЯДНТНЕКЦНШЕХЙЛКЙ  ШФМКЩЫЦЕНБЧЙЫЩИШНЦЦПНЩИШНЦУЫЭБСТЫФТТМУНИДЩСЙПЯНРУ  УФШТНКСФФРЙШУПКРЮЕСАУЧПЪУУЪЮФЙЧУЩДЫ_ФТШРЬРШЯПДПЪЖД  ЧОУЙЭЕЩДЭУИЕЪЙУЦШРДКЦНЬДЦЮУНТФДЧУУФЪЦЩМРОЕАЙЫФМКТУ  ТПНВУФОЫ_МОЕАЫМУЗЙЪХЮПЯЕЗШНВХТВБЙТЩБДПЪЖДТЫБИООУЗЙСБ  РШРЖДКНРЧТНЯВОЦУПШ_БХДВУГЙХШКЫЙУЗТФЖДЧУУРЗТЬДЦЮЧШНЬ  МЙЫЪЪЙЩТИНАКЙХАЕП_УНИЫЫПЪУТТШБИООУТПН_УРУЕДЛИЕАЙРУС  ШЯЮЗПНЦДЪ_ДШПМКЫ_ЦКЙСШКЙМУЖДЩУНИАЫТК_ПДШН_УПЪУФЪ  ЛКОЕЩСЙЦУТТШЕУЙЦЫДЪЧУЙЪХЮПЯЕЗКНАКЙАЫТКУЕДА_БДИНШКХО</p>

ядрццгйъщлоаубьц\_нйщсйеъьдтндумугэпыауйыбзшууйхмутпс  
бдааццьрьдырбжштодш\_узыучуйэгубушэпсбдшвцеьичехьукньу  
спфшшйкенццуиъах\_ццуцэжщцьрфстнюуьг\_янбтйрдчъукехнв  
уйтбхшсщдтнюуьг\_янакйэгнсыфзкщурзтпстнаеъоцтпнддырбн  
ццусшяюумяюнццумчоюуци\_ндщсйсгшлуцдлиядчогуонккцн  
\_кчйлкйпоршнвхтхаефьцд\_ццнхцые\_цьдью\_дырбжштакпнбтйджз  
ы\_цумоядыухгйяеемюбфшщпдающмйшбчшюоойбадоьялпыуж  
дщуфъьщмроеайъчуъдырйучуйрозпяюнйтфлпнзхкыйшссяюнпнц  
мудптншециузйшбрияюкйцызшхкнфцуцььтзбщдчоуфхьмеоцу  
жэщпзкюунйсбщцьшнчнцдбцакхцунйеягщууфъьиуоццэтчуфшн  
хшхйцеъаунйъчритщзбцэдщюбксфщишнхухйауйэбйпчдчмьцех  
цуткнакньусшфщчйпоченрчтнявоцумчосчйшбишнанлашайцыд  
цььйхаефь\_яньдпъждшэтченцщць\_ттцьценюрэпуфшюетшчуп  
кюе\_йяцкьнбчйяеемюбфшщтдсоеуйрдкйаъкйэбэхьушобцрп\_цую  
цекхйауйтыпшньдырщхянеуньуптьоднмьунйрбнчязепыауйцууху  
анчаузыууцъоаумцяуыйузпящрпуунйрщцщщкйрдкйшфмкшьд  
иъмнфцуццьехт\_щринюесояныйукцауфъьдчдъьдыамкы\_цеццуц  
йшбчшюостнщсэн\_урьбдлияуйэгуы\_бдбаеньйужпящйшрфченак  
йябулюфлкмупъьупйшфпшъждъобыхитждщюькттякрцедмящдщ  
юькттякроянйшухштждауяумуккышбсэнюуьг\_унх\_хнцкыйуж  
пядусыфчщптшн\_нхнбрпыьтэньдмящдоюжлпщсжчьууьыбцтщ  
ьценюдчу\_шйумкйрумпыякйрбоышфдоьяцфьчуйэщхпъщттщьды  
оанйыфдьякнауейхфды\_фзъьвуху\_дэфщды\_фршнеефнекщщбда  
\_бдшщтттыукяоядлуыдбах\_йпоркнжлпнцкыыфдчуьлттфтчотдм  
удкхотдмудткншриньрпыьткнауайсдэфщдчууфэяюехцунсндчк  
ььйцузпдщхшъуишрбхтщда\_бдшэфцчьузкысэкндчкщуфш\_гш  
бщцеьйунйюжлеуумкютлпыаупнякрояуйыфдщугкфщфйчьэдшщ  
щттыуцьоядпжщдмудкхуцдчоууобойяеечгьня\_уьюьчщпдъ  
одцфобыхнакооцтшндрэдъзбущциндчъолтшуушлцэцьрьдчоуйш  
юбипндчкщъдмяехпдфчечатдмьбхэфцтчищдхлшнйрбчйбауйсшк  
йыфьтыфкьятдньцуъцядыухкйьякчцадтнцпнъйкщузттфдыьщи  
шроъйсбхйэгуйшбчшюокйбауньуишрбхтщъдпъждштътйюфмйэ  
щхптузпдщхшъутшсфк\_нтсвцюдщщщчелушфобыхньмйхфдьяк  
дчоуишюодшщщтттыуцйффйчьдчелуцьоядмсягоицеьйдгйыьдли



	<p>ЯУЙЭФЦАГТШНЬДШПЯЕФОУЙШНВУХЫЦНЧИУМКЯЕНХОЯНИСБХДНБРПЫ          ЪТЭНЦНОЫЩРШЯПДА_БДЬУЦПЮБКЙПЩРШУУПЭЮКЕМЬЩДТНЮЕФНБТЙ          ЪЬДЫ_ФХКЩДГЙБАДЧУУСШСУТКЧЕНЙЬЬЬПСБДЯБГУБУЧУЙРУЗТТЩДНЬГ          ДЩЮБДФЬЕУЬИЩДШЫУЦЬЬЯАФЬУЬТ_ФРЙЦУЦХИЛЕХ</p>
19.	<p>ШЫПОЕДШЗПТЕРОЕМЮЩДЩАПЙФЦЙНЯРЫЧКАШЗПАДДЛЦРЕХЩЙНСРЬУ          ЪБТНЙЩЙФШБПРТЬТЦЕРСЕЙВПХПЫШСЙЭПЛОГЙЬПЗПТ_СЦНЙЮКДНАПЖ          ЧЦЙФПАМУЦРЯХПТЬКЙЬПЦТБЬ_ЯРНУЪРЛУХМБУУРАКАЮТДРЦМГЙЭПЛО          ГЙЬПЗПТ_СЦНЙЫКМКЫТДЩЦЪКЪЯОТТЬТЦЕРЫДЧЩЦНЙЩЙШЫУШНХЩЙЦ          ПТПДШТДЬКЩЙУЛАКМЙЧТМЧЩЙНЙЮЪЕМЛЙИША_КМРЧУЙГОКЪЧКРТРТ          ДЬСЦДМЯЙЗЫЦУДЩАПЛЧЦУДАЩЫЧШВПДЪГЫЦФЩУДИШДПЙЩЙЦЬСЪШ          ЗРМКЪГЙФЬЦОЕЧЩПДПЙПОДЯЙЦТЕЙФШАЙЦМЦРКПРЦКРХЭДФССЕФСЦН          ЙФШЗШАТЧЙЗЬУЙЖКХЕРТЗКЮЙИЪЯСТДЪЙФЬЩПМРСХДЧСЙЧПАПШЙУДМ          ДУКРЙБЙИЪЦЛТИРФДЫУШКЦГЙРТЖЭДЫВКХТЫШЗЙХКХТЫНЦРСКЦЪЗДЩ          ЯЙЦЗРЫЧШАШТЭРЪКФЩЙШМЦВКМСХДРЩБАЙУЙЙЪГРЖПРТДШТПЮКЪИТ          ПРЩХТЮЭЛОСЪАЙЩЯДЧЩЙПЙ_ШЙОСЧЪУЭДЧЩЙПЙ_ПХПЭТПРМКЪЛЙ          КВЦЙЙШРЫНЯРЩУЪРФЕСС_ПТЦЙХШХДДЫЗТЧКОБЦИРЬУОБЪЗШЭЙЦЙЗПЬ          ПНОЫПТЭТДТРХВЛЯМАЙЫЙЦМЯЛУОЦЙФЬССЙЧЯЫЧТРНХКТПЛЭРТДМЯУТ          ПРЫУЫВКЗХППЧЙФХЕМЮДКЙЗПХЪЛЙНЯРЯЕЪСФЧПАКДМЪТГЧЩПДЪЯЫЦ          ТЦЙЗДАКЛКЦЬЦИРЬУХМФУЙБЙТТПУДИШХЧУУРЫЧШАШТДРЫЧПБЧКЧЩПС          ЙУЙЗДТШХКЕЙЦЧПЬНПЭЙПШЫШПШЫШЗЙЩЙЗШЪЫПКЭТДФЯУЪЛПДЫВ          ШГЪРТДЩАШЪШХИЧЙВКСЙЫКМКЫЙФШРМРПЗПТТОЙСПЮПКЙЮПТКУТЙ          ТВЙЙРЦННЬСЙИША_ЕЙЫШЧШАДОЙГЛНХРПИШРЛХКВКДАЦЦДЫАХЙКВК          ДФЯУЪЛУДЫВШНЬРЭДЧЦНУЙЗЬУЛЛЙМКЙТЮКВЕДПФШДЫВКТТЖЭДЧЯЙ          ПШВШХДЪЙМКЫЭХТЪЙЧКТКПШЭЙКНЯЙЪКВЭДШЮЙШМСРЕПВЙЗЪСНЕЙ          ФШХ_СЙТШРЦХПШТХКЦЬДАГРУНЯЙЙХПЙТПФШДТРЭИЧЦЬЕЬЦХГЙБШРО          СЪЕЙБШЖЫВМКЧЮЩДЪГЫЦФЩУДЦГРНФРОРИРФЕССФЕЙЦЫЧЕРФЕФЯПД          БЯЙЪЭЧОУПРОНФЯПДТРЦХПШЪКЧЮШКЙБЭЮПБЪЗШРФУЪЯЪУНЯЙУЛАКМ          АЦФДШЮЙЗТХКРЙУЙМКЕШЙИЙТЪЙВШХНСБЕЯРТДЩЦЪКЫЦХКЧЖКЪЙЭК          РШАШЦЫЩИТКЕЙПШВШХДЕЙПКШКПТРЦХПШЪНЬЦХАЧАЙТКШДЗКОЪДБ          СЦУМСХЕЦЩЙЮПФШРЕБЪЗШРМДШХПЛОЦЙЦШБЬУТВЙЗЙ_ШЙЪСРЕЧЩТД          АЦЪППБЭДХГАЭПЦЙУЪГРНПРОУЛМЕПВЫГЙЯДНЯЪЫКРХШАИТКЙЬШЭК          ХТДЦЯФШЩСЗЧЫПЙНЙЫЪЕОГЬЦИРЭДЧЩЯДРЦЙСШЫШЙПЖЙПКШКПЙП          ИШЫИКЪРСТКЮТКЦРЬЕЪСЪЦФЯНУЙПС_ФСЙНИАКМНГХГМИТЦЕРОЕРЦЙЦЙ          БМУТЭЙЖЪСЪУЦРНУМЯЪНЬРЩУЙВКЧАЫПТРЧКЫЭШЧЪПЙТКРЬУЙНЬУЪР</p>

	<p>ЯХТБЪНКЮБПТЪЙТКАШЙПЖЙМКЫТТЭВДОЙУЙШНЯХУФРСКЦЪТДШЫЪШР  ЦТДЪЙФШЪЭЙТЫТСТРЦЕНЯЦКЪСЧЦФЩЦНЙ_ХКЦЦЧЕЦЦЙНЙБШРОСЪЕЦ  ЩЙЦАЩЪЕПВЙЦПТИДЧСЙЗДБШПШЪЙЦЫЦЦКЧЩЙХКШМНЬЩИДТРЦХТШ  ЧЕПВЙЪПЪШЗПЫШСЙВШРЕЫШДШХЧУНЯЙПКШКПКРЧЕЙУЫКЙЧПДШБЪЕХ  МЧУПРЫСШВЪНЬРЫДЩАПМЪЦНПЭЙПКШКПЙТШРЕИЭВЙЗКЦЪМЙЗЪЦЦК  ЧЩЙФЪЯМУОЩЪДЧСЙПШАОУЧСЯДМРЩУЯЯОЕЯРЧЕЙЯЯУЪЦЙНХЩЙХДТЧ  УУРХУМЪПДШЮЙФШЗЪНЙЮТПШФОЕЙЮПДЪСЛУЪСПЧЙХШСКРЦХПТДЗК  ЮТКЙЦНУЙУЙЦЪСЧН_ЦЙКЫВЕДТЪФРЗПТТЦЙНСРЦХКУТРКРЦХКШОТТЫ  ЙНЙВШИОСЙУЧРНШХППЧЙУТТШРЭДФССЕФЯМДЭРМЦПЕЙЦМЯПДТРЦАИ  ЮЫЧМЯЙКЫВЕДЧЦЙЦЪЯХАФЯЙУЛЙКГЙУЫКЦРЫПХЯЧТШБЪАЙБФУХМФУ  ЙЯЛХИХЙТПЩЫФШЪЧКЧЩПДФЯЪУЪЯНУЙБШЪХЯЯАЙТДДСЙУЪБЪШЩЮ  ТЪПЪЗШРЧЕЙЧПТВЩЧШЙЫКМКЫЙЦЦЯЪХТВЙПКЫЙТКРШХЭХТКЙБМУПФ  ЩДЪЛКИШБШЩЪЯИТТПЙЙПУФКЙВШРЕЫШДЩЯСЗШЫКЪРНШХПЪАЙТКЖЭ  РРКЙШКЦЪСМРИЦЪДЫРЦУХЯОУЫВТДТРОУЙФХШЛЯФУУРЫЧКАШЦЪЩЙХК  ТШЧКВЕДОБИДЪЦЛГЙЩЙЦЦЯЪХТВЙТКРРКЧЙТТЭРЫДМЯЫЧШЗЧ_ЦРЪХПТ  ШЗКЮТКЦРЩУФЯЪТШБЪНЙЩЙЧЪГОЕЙУЫРПХЫЧМЩПДЪСФУНЯЙЗСФХГО  СЙЛПЮВНЧСЙШЫЩХКЧЮЩДЪССЗТУКГЫМЙНЙДТМТЗПЦФЩЙНЙЮЪЕМЪ  ЗПЮЧУЙЕШЧИРТДЩЯФУЪПИЦЕРЧЕЪГРТШРЩУХГАЕПВЙПКЫЙЗШЯЛЮПРЧ  ЕЙУЩЦЪЯФКЙТПМЙЪЕМЮПТТПЙЖШЪЕЭПЦЙЪПЭЙТКРСЕЦСОКЙУХНИЮ  ТКЙЩЙЗПЪЙЗЙХШСКИЧКЦРЛ_ЪГ</p>
20.	<p>МЕКЪКЦЕМШ_УЯККЗМЩЦРТЙЮЗХОРРХЙЩРТЧЙДХЙЪУЮФЛПНХУДЧЙШК  ЩЭКЦЯШУЧМШЦКЪЕКИЫХЩЗ_ЙЪУСЧЙРМЧЛДЫЯЩЧ_ЙЩИШИП_ПКРЧЮИ  КЖ_ОЭУМРПКЯЙБКРШКЧЫЙШКММУЙНХКЧНФЩИЫЙТЗТЪЙДХЙЪЕЩЙЛИР  ПФДЭШЪРЗУКНМНЦЕСФУОМЦЦХСККЧЫЧХЕЛЙЮСЪКЙДЭШОЕМФЛПМОРХ  ТМЩДППЭЗХЫЭУТЙЩЧМФЩТВККЙЫЙХУЪ_ЛДВПЦЕЛЙЪЕУПШАМБРХЮБЖ  ДРЧРЙНИКЖШПЪЧХЪКПНФКРЫВРТНИКРЛРХНМЛРРЗПКПНФКЦЪПОДЮФЛЬ  ТЪКПМЧРС_ЙЛИРПФДХЙПНПТЭЦЛЙБЧЫЙШКМЭ_УСТЭДЫХРТИЙЛДЪККТТН  ЩДПЫРДЮЦЦЧЭТЭДОЩЦАДТЧНМНЦЕФКЧНМЪЦЪЪШКЦЧКТЕЯЕКЪЯШКЧ  ЫЙ_УГПЭДЫШПЦКХЕШЙЛИРПФДСЭЧЕШЙЮЛМФЩФИПКСТЫШШЯЕКФЫМ  РХЪЭЦЦЛЙТЗТЪЖДПСЧЕБЧЮРММРЧПТЬЧЗЦУДЭШОЕЩТКФЭИШШШЙЪКЭ  МЕСМЫХУЧШЧДЪККЧЭТКЦНРРТХЙУДЫШВКШЙЪУМЩЦРКЙХУЪЕКЖЗХКШ  МКОИТИКЧНФЩОМАЭУМТКЫТЧЕДТЦЮДЪПКЖЗХЩДНЙЧНХКУЯЫЭЕПКЭ  АМШМКЭЧЮРЮИКФЭКННЯПЦАМЧЛДЮМЩНБЙЩЪЪШНЧШНДНЙУЪМЭС  КМПЗНЙУДПТПТЪЙЪУЮЦЩЧЭПЦДПЩРХТОКТНЙЩРТЧЙДХЙННСТЭДГЪ</p>

ЩДФМРХИЙЪУДПЦДЯТВКМЧЮДСЭЧЕТЪКЙЫНЦТКЙЬПНАРЧММЩДПЫИДЧ  
ШЩЦЭИДЩШБАМТКЗХОУЧММЬКМЛЦНУПКНМЛЦНУПКПМЧРС\_ЙМКШДР  
ДШИСПХЙЩРТЧЖНМЦРРИФЛВЯЙЭУШЕХУМЯЩЧТХКЖЗХЩДЧШЪАТЙМХЫ  
ЫУЧИЙЩРТЧЖДЫЛРХЪЭЦДРЩЦУПЭКТНОПЕШЙЩФЛЬЖДННОКЦЙПЕШПХ  
УМШЭДЪПОУМШ\_УЯДКШУПКЙНМШУМЧРДПТПТЪЙУДЮФЛЬ\_БКЗМАУЦЯ  
ШЧДЪШЦКМЬЩРИФЩДЫХРТИЙПЕМКОИТУКТНЙХУЪПКИЫЧЙРЮИКУЪЙТЕ  
МЧУСМЩЦРСЧЙДПТПНЯЙШЕЧШШКВЙБЧЫЙЩРТЧЖДЧЙЫКЧПКЖТРУЧМЧ  
ЮДСЭЧЕТЪККЮХУДЪКЪХНМЩДЪШФЙТЬКФЭШЪЕШЙЛДЪКЦКПШКСЫУКТ  
НХРЗЫЙЫКЧКР\_ФЮДЮОРРНХЛДХЙШКЧЭПЕМСНКЭЗКЖЗХЩДЫЪЭШСКК  
ШЦЪУДЮСЛЙХЙЩЪЫЪШНЧЙЪФТЪРЙХЙЫКЧККЭХЪЦПНИКТХЙБКШШНКЧ  
ЭКТХЙТЗТЪИДЪПКФТЪРФЩДЭАМЩЦЗТЪШШШЙЩРТЧЖДЪКЦКПШКМНОЫ  
УУКЦУМЭКЕРНРГМЫРХС\_РДЫЪКХНОЦЦЯТКЦЧКБКЯЙЛДЮКЧДСЭЧЕТЪКЦЧ  
ШЫУМЪРПНЙШКЧЭПЕМЪРЖТЙЮОЯТКФЫОБПНФЛРМШЦКЪЕКПМЛРХТНЮ  
ДНЙШКСКЦКЧШКУЯЙМКЭПОЕМШЪЧЭШНУЧЙШКОЩЦАДШФДНЙШЕМШЪЧ  
ЭШНКМФЮЦЯДКИ\_ЫЭ\_ТЙУДШПЪДЦПЦПХУКФЭДОТ\_ХКУШПШАМЬЩДП  
ЫРИЫЙЫЕФЦЛЪНЙНДПШПШМШХШЪЭЦЦЛЙН\_ЪДЫТ\_ХКНМЩЦФЩДЦДЪ  
ККУЮЫУПЙЪУСЫХЕЧКЦДННОКЦЙУДПТПНЯЙБЧЫЙТЗТЪЖДПЙХШЮБЕД\_  
БРРМЩЦИЪКЦДХЙЩТМФЦТЛЙНДПШПШМЫЭШЪТЦДЧШШАММКЗЫОЮДД  
КОТ\_ХКЧЭТКХНСЛДХЙЮЭТХКЗММЩЦЙ\_ЙЪУМБРВМККЙНХЖЭТЙШУРКНМ  
ОШЕМЧРДСШЪЧНПЭДЪШНКЭЧЮРМКОИТУКТНСЛЙМЧЛДОПЫКРЙПШЦКРЧ  
МЩЦКЪЕКУЯЙЧКЪИКНМЬЛПМЧРД\_УПКЯЙЛДЪККЧНФЩОМЛЕЦЯЪУТТЙЪУ  
УКЦЩЦЙУДЧШШГМЭЭУЪТВАМЬЦКФЙЪДЧШШГМЦЫНПИТЕШЙРИЫЙХДЧ  
ЭЪЧ\_ЙЪТЛХКЦМЫРЖЛЙПУЭШОУТЙЪРНЪЖКМТКФЫБРРММКЗЫОЮДЪХЕРМ  
ЩЦ\_ШЙРЙПККТТЙЮТТЫЦУМЧЛПЫЧРЫМЩЦФЭШМУПКЦДЪШОУЦЙПТЪЙ  
ШШМОЮСНПЭДЮПФЪНЫКГМПОУМОЩЦЯКШШМТКФЫБРРММКП\_ЫЭ\_МЪ  
ЛМРЧРЗНХЪГМНЦЦЪШПАМЧЛДННОКЛЙЪХХСНЕСШЙЩТМФКЦТЛРДНЧОКШ  
ККНМЩЦЦЗТХРРМПЧШМЩЫНЪИНДЪККЦТЛЙДПТПДННОКТМКУСПЭАЮИКЗ  
МПОУМЩЦЕЯЕРДЮПЪЧИЙШЕМФЦТЛЙУДТЯЛЧИЙНДРШЫУСЙУДХЫЪУШЧ  
УРМКШИТХКЗЫХИДРШЪФЫОШВМЩЦДЮХЩЗ\_ЙРИЫЙУЦКЦДХЫХЕШЙТЗ  
ТЪЙДННОКЦЙЪУМФЮЦЯКЧДЪПЭДФМРХЛЙНКЮЕКУЮЫУПЙХХ\_НЦСМШ  
МУДПЦДЪШЪКЭПХДЮФНУФЕКП\_ЫЭ\_МТТРНСУРМЧРЧМЧУЪТНЩДХЙШКМ  
ЩЫНСЭЧЕТЪКЕРНРОМФЮЙНЙПКПКЦЦЛЙЩРТЧЖДПЩЦРХТОУДЭПХЕМБУХ  
ЫФЛГМЧУПНФЦС\_ЙТЗТЪИДЪПКФТЪРФЩДЭАМОЛДХЙЮЗХОРРМЛЕДЫЧКУ  
ШПШГМПЪРХЙМ\_МЫЩЧМЩЦФЩДЭАММТЙ\_ЦЛРМОЩЦНОШУМЫЭЕШШК

ЕРНРВМШПТНФЦДСПЦЕЯЕКТАРИЙШЕСШКТНСЛЙММЦХЫАЛЧИЫЙДЫ ЧКЗЗБРРМФКЗЫОРДОЪЩЦХХКПЫЩЖКМАЭУОЙШКМЦРЭНХЩДХЙЪХХЩЦ ШЙХДОПЫКРЭКЦЩШЭХХЬКТХЙХУЪИКТХЙЪРНЬЖГМЧРЧ
--

### **Содержание отчета**

- 1) Титульный лист (Пример в приложении В).
- 2) Цель работы.
- 3) Таблицы, вычисления, примеры расчетов.
- 4) Зашифрованный и расшифрованный текст.
- 5) Выводы.

### **Контрольные вопросы**

- 1) Опишите как получается матрица Виженера.
- 2) Опишите методику шифрования текста шифром Виженера.
- 3) Опишите методику нахождения длинны ключевого слова.
- 4) Опишите методику нахождения ключевого слова если известна

его длинна.

### **Литература**

1) Титов, А. А. Инженерно-техническая защита информации: учебное пособие / А. А. Титов. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/13931.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

2) Литвинов, Р. В. Технические средства защиты информации. Часть 1: курс лекций / Р. В. Литвинов, К. А. Волегов, А. П. Бацула. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2006. — 170 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/14027.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

3) Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 95 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17925.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

4) Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 104 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17926.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

**Тема 4. Методы защиты информации с применением  
симметричных алгоритмов шифрования**

**Лабораторная работа №3 «Изучение математической модели  
симметричного алгоритма шифрования на примере XOR и  
численного метода его реализации»**

**Цель работы:** изучить алгоритм шифрования XOR при использовании закрытого ключа, построить его математическую модель.

**Программа работы**

- 1) Изучить теоретический материал, математические и алгоритмические особенности шифра XOR.
- 2) В соответствии с заданием построить математическую модель кодирования и декодирования текста.

**Элементы теории**

XOR – это логическая функция булевой алгебры, другое ее название исключающее или, эта логическая функция, как и любая другая используется для работы с данными, представленными в двоичной системе исчисления. Основным достоинством, позволяющим использовать эту функцию в алгоритмах шифрования, является ее обратимость, при отсутствии потери информации.

Как ни странно, но самым простым и одним из самых эффективных (при правильном использовании) алгоритмов шифрования является так называемое XOR-шифрование. Как известно из булевой алгебры, операция логического сложения по модулю 2 « $\oplus$ » (или логического исключающего ИЛИ — XOR, eXclusive OR) имеет следующую семантику (таблица 3.1) то есть, операция  $z = x \oplus y$ , по сути, поразрядная (побитовая — результат не зависит от соседних битов).

Таблица 3.1 – Таблица истинности для логической операции XOR

X	Y	$X \oplus Y$
0	0	0
0	1	1
1	0	1
1	1	0

Воспользовавшись таблицей 3.1, рассмотрим пример применяя операции сложения по модулю 2 для двух десятичных чисел  $X=10$  и  $Y=12$ .

Представим  $X$  и  $Y$  в двоичной системе счисления:  $X=1010$  и  $Y=1100$ .

Тогда

$$\begin{array}{r}
 X = 1010 \\
 \oplus \\
 Y = 1100 \\
 \hline
 Z = 0110
 \end{array}$$

Как видно из приведенного примера можно восстановить одно из слагаемых при помощи второго.

Из этого следует что алгоритм XOR это алгоритм с симметричным шифрованием, то есть для шифрования и дешифрования используется один и тот же ключ.

### **Пример применения алгоритма XOR**

Ниже рассмотрен пример алгоритма XOR для заданного фрагмента текста. Так как логические операции применяются для чисел в двоичной системе счисления то представленный текст необходимо преобразовать в виде набора двоичных символов. Для этого можно применять различные таблицы символов. В рассмотренном примере была применена таблица символов ASCII (Приложение Б).

В качестве примера использовалось четверостишие стихотворения А. Блока:

Ночь, улица, фонарь, аптека,  
 Бессмысленный и тусклый свет.  
 Живи ещё хоть четверть века —  
 Всё будет так. Исхода нет.

Алгоритм шифрования, следующий:

1) применить таблицу символов (например ASCII приложение Б), и получить соответствующие значения (Таблица 3.2);

2) код символа преобразуется в двоичную систему счисления (Таблица 3.3);

3) так как в таблице ASCII используются числа длиной 8 bit, то для простоты вычислений и пояснения следует применять ключ не более 8 bit. В примере рассмотрен ключ KEY=70 который в двоичной системе KEY=1000110. Применив операцию сложения по модулю два (XOR) получим следующее сообщение (таблица 3.4);

4) далее сообщение из двоичной системы счисления преобразуется переводится в десятичную (таблица 3.5);

5) используя таблицу ASCII кодов зашифрованное сообщения из числового кода преобразуется в текстовое сообщение (таблица 3.6).

В результате после всех операций получится следующее зашифрованное сообщение:

«Ë±ejfµ-®°|jfiË«|¶ejf|©rJ-!j  
‡J··CS·-J««Sİf®frµ·-Sİf·¤Jrh  
Ъ®¤®fJiüofiËref±Jr¤J¶ref¤J-!fC  
„·üof§µÿJrfr|~hfñ·iËÿ|f«Jrh

Обратная процедура проводится в этом же порядке.



Таблица 3.2 – Результаты замены символов на цифры

Символ	Н	о	ч	ь	,		у	л	и	ц	а	,		ф	о	н	а	р	ь	,		а	п	т	е	к	а	,				
Код символа	2 0 5	2 3 8	2 4 7	2 5 2	4 4 4	3 2	2 4 3	2 3 5	2 3 2	2 4 6	2 2 4	2 4 4	4 4 4	3 2	2 4 4	2 3 7	2 2 4	2 4 0	2 4 2	4 5 2	3 2	2 4 4	2 3 9	2 4 2	2 2 9	2 3 4	2 2 4	2 2 4	4 4 4			
Символ	Б	е	с	с	м	ы	с	л	е	н	н	ы	й		и		т	у	с	к	л	ы	й		с	в	е	т	.			
Код символа	1 9 3	2 2 9	2 4 1	2 4 1	2 3 6	2 5 1	2 4 1	2 3 5	2 2 9	2 3 7	2 3 7	2 5 1	2 3 3	3 2	2 3 2	2 2	2 4 2	2 4 3	2 4 1	2 3 4	2 3 5	2 3 1	2 3 3	2 5 1	2 3 2	2 4 1	2 2 6	2 2 9	2 2 4	2 2 9	2 4 2	4 6
Символ	Ж	и	в	и		е	щ	ё		х	о	т	ь		ч	е	т	в	е	р	т	ь		в	е	к	а		—			
Код символа	1 9 8	2 3 2	2 2 6	2 3 2	3 2	2 2 9	2 4 9	1 8 4	2 3 2	2 4 5	2 3 8	2 4 2	2 4 2	2 5 2	3 2	2 4 7	2 2 9	2 2 6	2 2 9	2 4 0	2 4 2	2 4 2	2 5 2	2 2 6	2 2 9	2 3 4	2 2 4	2 2 4	2 3 4	2 2 4	3 2	1 5 1
Символ	В	с	ё		б	у	д	е	т		т	а	к	.		И	с	х	о	д	а		н	е	т	.						
Код символа	1 9 4	2 4 1	1 8 4	3 2	2 2 5	2 4 3	2 2 8	2 2 9	2 4 2	2 4 9	3 2	2 4 2	2 2 4	2 3 4	4 6	3 2	2 0 0	2 4 4	2 3 8	2 2 8	2 2 4	3 2	2 3 7	2 2 9	2 4 2	4 6						

Таблица 3.3 – Код символа в двоичной системе счисления

Код символа	2 0 5	2 3 8	2 4 7	2 5 2	4 4 4	3 2	2 4 3	2 3 5	2 3 2	2 4 6	2 4 4	4 4 4	3 2	2 4 4	2 3 8	2 3 7	2 2 4	2 4 0	2 5 2	4 4 4	3 2	2 4 4	2 3 9	2 4 2	2 2 9	2 3 4	2 2 4	4 4 4					
Код символа в дв. сист. числ.	1 1 0 0 1 1 1	1 1 0 0 1 1 0	1 1 1 0 0 1 0	1 1 1 0 0 1 0	0 0 1 0 0 0 0	0 0 1 0 0 0 0	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	0 0 1 0 0 0 0	0 0 1 0 0 0 0	0 0 1 0 0 0 0	1 1 1 0 0 0 0	1 1 1 0 0 0 0	1 1 1 0 0 0 0	1 1 1 0 0 0 0	1 1 1 0 0 0 0	0 0 1 0 0 0 0	0 0 1 0 0 0 0	0 0 1 0 0 0 0	1 1 1 0 0 0 0	1 1 1 0 0 0 0	1 1 1 0 0 0 0	1 1 1 0 0 0 0	1 1 1 0 0 0 0	1 1 1 0 0 0 0	0 0 1 0 0 0 0	0 0 1 0 0 0 0	0 0 1 0 0 0 0	0 0 1 0 0 0 0	0 0 1 0 0 0 0

Код символа	1 9 3	2 2 9	2 4 1	2 4 1	2 3 6	2 5 1	2 4 1	2 3 5	2 2 9	2 3 7	2 3 7	2 5 1	2 3 3	3 2 2	2 3 2	3 2 2	2 4 2	2 4 3	2 4 1	2 3 4	2 3 5	2 5 1	2 3 3	3 2 1	2 4 1	2 2 6	2 2 9	2 4 2	2 4 2	4 6 6
Код символа в дв. сист. счисл.	1 1 0 0 0 0 1	1 1 0 0 1 0 1	1 1 1 0 0 0 1	1 1 1 0 1 0 1	1 1 0 1 0 1 1	1 1 1 0 0 1 1	1 1 1 0 0 1 1	1 1 0 1 0 1 1	1 1 0 0 1 0 1	1 1 0 1 0 0 1	1 1 0 1 0 0 1	1 1 1 1 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 0	0 1 0 1 0 0 0	0 1 0 0 0 0 0	0 0 1 0 0 0 0	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	0 1 0 0 0 0 0	1 1 0 0 0 0 1	1 1 0 0 0 0 0	1 1 0 0 0 0 0	1 1 0 0 0 0 0	0 0 1 0 0 0 0
Код символа	1 9 8	2 3 2	2 2 6	2 3 2	3 2 9	2 4 9	2 4 9	1 8 4	3 2 2	2 4 5	2 3 8	2 2 2	2 4 2	3 2 2	2 4 7	2 2 9	2 2 6	2 2 9	2 4 0	2 4 2	2 4 2	2 5 2	3 2 2	2 2 6	2 2 9	2 2 4	2 2 4	3 2 2	1 5 1	
Код символа в дв. сист. счисл.	1 1 0 0 0 1 0	1 1 1 0 0 1 0	1 1 1 0 0 0 0	1 1 1 0 0 0 0	0 1 1 0 0 1 1	1 1 1 0 1 0 0	1 1 1 0 1 0 0	1 0 1 1 0 0 0	0 0 1 1 0 0 0	1 1 1 0 1 1 0	1 1 1 0 1 0 0	1 1 1 1 1 0 0	1 1 1 1 1 0 0	1 1 1 1 1 0 0	0 1 0 0 0 1 0	0 1 0 0 0 0 1	1 0 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	0 1 1 0 0 0 0	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	0 0 1 0 0 0 0	
Код символа	1 9 4	2 4 1	1 8 4	3 2 5	2 2 3	2 4 8	2 2 9	2 2 2	2 4 2	3 2 2	2 4 2	2 2 4	2 3 4	4 6 4	3 2 0	2 0 1	2 4 5	2 4 8	2 2 8	2 2 4	3 2 2	2 3 7	2 2 9	2 2 2	2 4 4	4 6 6				
Код символа в дв. сист. счисл.	1 1 0 0 0 0 0	1 1 1 0 0 0 0	1 0 1 0 0 0 0	0 0 1 0 0 0 0	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 0	1 1 1 0 0 0 0	0 1 1 0 0 0 0	1 1 1 0 0 0 0	1 1 1 0 0 0 0	1 1 1 0 0 0 1	0 0 1 0 0 0 1	0 0 0 0 0 0 0	0 1 0 0 0 0 0	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	0 1 0 0 0 0 0	1 1 1 0 0 0 1	1 1 1 0 0 0 1	1 1 1 0 0 0 1	0 0 1 0 0 0 0		

	1	0	0	0	0	1	0	0	1	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	1	1	
	0	1	0	0	1	1	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0

Таблица 3.4 – Зашифрованное сообщение

Код символа в дв. сист. счисл.	1	1	1	1	0	0	1	1	1	1	1	0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	0		
	1	1	1	1	0	0	1	1	1	1	1	0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	0		
	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	0	0	1	1	0	0	1	0	0	1	0	0	0	1	0	0	0	1	1	0	0	0	0	1	0	0	0		
	1	1	0	1	1	0	0	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0	1	0	0	1	0		
	1	1	1	1	1	0	0	0	0	0	1	0	1	0	1	1	1	0	0	1	1	0	0	1	0	0	1		
	0	1	1	0	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	0		
Операция XOR	1	1	1	1	0	0	1	1	1	1	1	0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	0		
	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	1		
	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	0	0	1	1	0	0	1	0	0	1	0	0	0	1	0	0	0	1	1	0	0	0	0	1	0	0	0		
	1	1	0	1	1	0	0	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0	1	0	0	1	0		
	0	0	0	0	0	1	1	1	1	0	1	0	1	0	0	0	1	1	0	0	1	1	0	1	0	1	0		
	1	0	0	1	1	1	0	0	1	0	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	0	1		
Код символа в дв. сист. счисл.	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	1	1	1	0	1	1	1	0	
	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	1	1	1	0	1	1	1	0	
	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
	0	0	1	1	0	1	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0	1	0	0	1	0	0	1	0
	0	0	0	0	1	1	0	1	0	1	1	1	1	0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	
	0	1	0	0	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	
	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	0	1	1	0	1	1	1	0	0	0	1	1	
Операция XOR	1	1	1	1	0	1	1	1	1	1	1	1	0	0	0	0	1	1	0	1	1	1	0	1	0	1	0		
	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	1		
	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	0	0	1	1	0	1	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0	1	0	0	1	0	0		

	0	0	0	0	1	1	0	1	0	1	1	1	1	0	1	0	0	0	0	1	1	1	1	0	0	0	0	0	1	
	1	0	1	1	0	1	1	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	
	1	1	1	1	1	0	1	0	1	1	1	0	1	1	1	1	0	0	1	0	0	0	1	1	1	0	1	0	0	
	1	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	0	1	1	0	1	1	1	1	0	1	0	1	0	
Код символа в дв. сист. счисл.	1	1	1	1	0	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	0	1	
	1	1	1	1	0	1	1	0	0	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	0	0	
	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	
	0	0	0	0	0	0	1	1	0	1	0	1	1	0	1	0	1	0	0	1	1	1	0	0	0	0	0	0	1	0
	0	1	0	1	0	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	
	1	0	0	0	0	1	0	0	0	0	1	1	0	1	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1	0
	1	0	1	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	1	0	0	1	0	0	1	0	1	0	1	0
	0	0	0	0	0	1	1	0	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	1	0	0	1	
Операция XOR	1	1	1	1	0	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	1	0	1	
	0	0	0	0	1	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	
	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	
	0	0	0	0	0	0	1	1	0	1	0	1	1	0	1	0	1	0	0	1	1	1	0	0	0	0	0	0	1	0
	0	1	0	1	0	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	
	0	1	1	1	1	0	1	1	1	1	1	0	0	1	0	0	1	1	0	1	1	0	1	1	0	1	1	1	1	0
	0	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	0	0	1	1	0	1	1	0	1	0	1	1	0	
	0	0	0	0	0	1	1	0	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	
Код символа в дв. сист. счисл.	1	1	1	0	1	1	1	1	1	0	1	1	1	0	0	1	1	1	1	1	1	0	1	1	1	0				
	1	1	0	0	1	1	1	1	1	0	1	1	1	0	0	1	1	1	1	1	1	0	1	1	1	0				
	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1				
	0	1	1	0	0	1	0	0	1	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0			
	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	0	1	0	0	1			
	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0	0	1	1	1	0	0	1	1	0	1				
	1	0	0	0	0	1	0	0	1	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	1	1				
	0	1	0	0	1	1	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0					
Операция XOR	1	1	1	0	1	1	1	1	1	0	1	1	1	0	0	1	1	1	1	1	1	0	1	1	1	0				
	0	0	1	1	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0	1				
	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1				
	0	1	1	0	0	1	0	0	0	1	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	1				

	0	0	1	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	0	1	0	0	1	
	1	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	0	0	0	1	1	0	0	1	0	
	0	1	1	1	1	0	1	1	0	1	0	1	0	0	1	1	1	1	0	1	1	1	1	1	1	0	0
	0	1	0	0	1	1	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0	0	

Таблица 3.5 – Перевод зашифрованного сообщения из двоичной системы счисления в десятичную

Операция XOR	1	1	1	1	0	0	1	1	1	1	1	0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	0
	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	1
	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	1	1	0	0	1	0	0	1	0	0	0	1	0	0	0	1	1	0	0	0	0	1	0	0	0
	1	1	0	1	1	0	0	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0	1	0	0	1	0
	0	0	0	0	0	1	1	1	1	0	1	0	1	0	0	0	1	1	0	0	1	1	0	1	0	1	0
	1	0	0	1	1	1	0	0	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	0	0	1	1
1	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	
Зашифр. сообщ. в дес. сист. счисл.	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	3	6	7	8	0	0	8	7	7	7	6	0	0	7	6	7	6	8	8	0	0	6	6	8	6	7	6
	9	8	7	6	6	2	1	3	4	6	6	6	2	8	8	1	6	2	6	6	2	6	9	0	3	2	6
	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1
	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0
	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	1	1	0	1	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0	1	0	0	1	0	0
0	0	0	0	1	1	0	1	0	1	1	1	1	0	1	0	0	0	0	1	1	1	1	0	0	0	0	
1	0	1	1	0	1	1	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	
1	1	1	1	1	0	1	0	1	1	1	1	0	1	1	1	1	0	0	1	0	0	0	1	1	1	0	
1	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	0	1	1	0	1	1	1	0	1	0	0	
Зашифр. сообщ. в дес. сист. счисл.	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	3	6	8	8	7	8	8	7	6	7	7	8	7	0	7	0	8	8	8	7	7	8	7	0	8	6	6
	5	3	3	3	0	9	3	3	3	1	1	9	5	2	4	2	0	1	3	2	3	9	5	2	3	4	3

Операция XOR	1	1	1	1	0	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	1	0	1	1	1	1	0	1		
	0	0	0	0	1	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	1		
	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0		
	0	0	0	0	0	0	1	1	1	0	1	0	1	1	0	1	0	1	0	0	1	1	1	0	0	0	0	1		
	0	1	0	1	0	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0		
	0	1	1	1	1	0	1	1	1	1	0	0	1	0	1	0	0	1	1	0	1	1	0	1	1	0	1	1		
	0	1	0	1	1	1	1	1	1	1	0	0	1	1	0	1	0	0	1	1	0	1	1	0	1	0	1	0		
Зашифр. сообщ. в дес. сист. счисл.	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2		
	2	7	6	7	0	6	9	5	0	7	6	8	8	0	7	6	8	6	6	8	8	8	0	6	6	7	6	0		
	8	4	4	4	2	3	1	4	2	9	8	0	6	2	7	3	0	4	3	2	0	6	2	4	3	2	6	2	9	
	Операция XOR	1	1	1	0	1	1	1	1	1	0	1	1	1	0	0	1	1	1	1	1	1	0	1	1	1	0			
		0	0	1	1	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0	1			
		0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1			
		0	1	1	0	0	1	0	0	1	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0		
0		0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	0	1	0	0	1			
1		1	1	1	1	1	0	0	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	0	0	1	0			
0		1	1	1	1	0	1	1	0	1	0	1	0	0	1	1	1	1	0	1	1	1	1	1	1	0	0			
Зашифр. сообщ. в дес. сист. счисл.	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1				
	3	8	5	0	6	8	6	6	8	0	8	6	7	0	0	4	8	7	6	6	6	0	7	6	8	0				
	2	3	4	2	7	1	2	3	0	2	0	6	2	4	2	2	3	9	8	2	6	2	1	3	0	4				

Таблица 3.6 – Перевод зашифрованного сообщения в текстовый формат с применение ASCII таблицы

Зашифр. сообщ. в дес. сист. счисл.	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
	3	6	7	8	0	0	8	7	7	7	6	0	0	7	6	7	6	8	8	0	0	6	6	8	6	7	6	0	
	9	8	7	6	6	2	1	3	4	6	6	6	2	8	8	1	6	2	6	6	2	6	9	0	3	2	6	6	

Символ зашифр. сообщ.	<	Ё	±	ε	j	f	μ		®	°	¡	j	f	I	Ё	«	¡	¶	ε	j	f	¡	©	r	J	¬	¡	j	
Зашифр. сообщ. в дес. сист. числ.	1 3 5	1 6 3	1 8 3	1 8 3	1 7 0	1 8 9	1 8 3	1 7 3	1 6 3	1 7 1	1 7 1	1 8 9	1 7 5	1 0 2	1 7 4	1 0 2	1 8 0	1 8 1	1 8 3	1 7 2	1 7 3	1 8 9	1 7 5	1 0 2	1 8 3	1 6 4	1 6 3	1 8 0	1 0 4
Символ зашифр. сообщ.	‡	J	·	·	Є	S	·		J	«	«	S	İ	f	®	f	r	μ	·	¬		S	İ	f	·	α	J	r	h
Зашифр. сообщ. в дес. сист. числ.	1 2 8	1 7 4	1 6 4	1 7 4	1 0 2	1 6 3	1 9 1	2 5 4	1 0 2	1 7 9	1 6 8	1 8 0	1 8 6	1 0 2	1 7 3	1 6 0	1 8 4	1 6 3	1 8 2	1 8 0	1 8 6	1 0 2	1 6 4	1 6 3	1 7 2	1 6 6	1 0 2	2 0 9	
Символ зашифр. сообщ.	Ђ	®	α	®	f	J	ï	ю	f	i	Ё	r	ε	f	±	J	r	α	J	¶	r	ε	f	α	J	¬	¡	f	C
Зашифр. сообщ. в дес. сист. числ.	1 3 2	1 8 3	2 5 4	1 0 2	1 6 7	1 8 1	1 6 2	1 6 3	1 8 0	1 0 2	1 8 0	1 6 6	1 7 2	1 0 4	1 0 2	1 4 2	1 8 3	1 7 9	1 6 8	1 6 2	1 6 6	1 0 2	1 7 1	1 6 3	1 8 0	1 0 4			
Символ зашифр. сообщ.	„	·	ю	f	§	μ	ÿ	J	r	f	r	¡	¬	h	f	Ђ	·	i	Ё	ÿ	¡	f	«	J	r	h			

## **Указания по технике безопасности**

В начале каждого семестра, со студентами должен проводиться инструктаж по технике безопасности в лаборатории. Во время нахождения студента в лаборатории и выполнения лабораторных работ студент не должен нарушать инструкции по охране труда с персональным компьютером ИОТ-37-ИВЛ-19, и инструкцию о мерах пожарной безопасности ИБП-01-2016.

## **Методические указания к выполнению работы**

Каждому студенту необходимо зашифровать и расшифровать текст полученный в первой работе.

При выполнении работы разрешается использовать любые технические и программные средства.

## **Содержание отчета**

- 1) Титульный лист (Пример в приложении В).
- 2) Цель работы.
- 3) Таблицы, вычисления, примеры расчетов, диаграммы.
- 4) Зашифрованный и расшифрованный текст.
- 5) Выводы.

## **Контрольные вопросы**

- 1) Опишите методику шифрования с закрытым ключом.
- 2) Опишите логическую операцию XOR.
- 3) Механизм работы шифрования на основе XOR.
- 4) Насколько надежен рассмотренный алгоритм шифрования на основе XOR?

## **Литература**

1) Титов, А. А. Инженерно-техническая защита информации: учебное пособие / А. А. Титов. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/13931.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей



2) Литвинов, Р. В. Технические средства защиты информации. Часть 1: курс лекций / Р. В. Литвинов, К. А. Волегов, А. П. Бацула. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2006. — 170 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/14027.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

3) Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 95 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17925.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

4) Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 104 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17926.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

## **Тема 5. Методы защиты информации с применением асимметричных алгоритмов шифрования**

### **Лабораторная работа №4 «Изучение математической модели асимметричного алгоритма шифрования и численного метода его реализации на примере алгоритма RSA»**

**Цель работы:** изучить принцип работы алгоритмов шифрования открытым ключом (асимметричных алгоритмов) на примере алгоритма RSA.

#### **Программа работы**

- 1) Изучить теоретический материал, математические и алгоритмические особенности шифрования с открытым ключом.
- 2) В соответствии с заданием построить математическую модель кодирования и декодирования текста с использованием алгоритма RSA.

#### **Элементы теории**

Основной трудностью при использовании симметричных алгоритмов шифрования в защите данных является безопасное распределение ключей. Для защищенного обмена данными между двумя сторонами, одна из сторон схемы обмена сообщениями должна сгенерировать ключ и конфиденциально передать другой, что достаточно проблематично безопасно сделать.

В связи с тем, что современный пользователь все больше и больше использует цифровое пространство, в том числе хранит свои персональные данные в сети, становится активным пользователем цифровой экономики то проблема защиты данных играет важную роль, а следовательно проблема безопасной передачи ключа при симметричном шифровании становится все сложнее.

В связи с вышесказанными возникла необходимость разработки методов защиты информации отличающихся от симметричных алгоритмов по принципу действия. Одним из таких методов это использование алгоритмов с открытым ключом, метод которого был предложен в 1976 г. Уитфилдом

Диффи и Мартином Хеллман в работе «Новые направления в современной криптографии».

Суть алгоритмов с открытым ключом основана на том, что для процессов шифрования и дешифрования используются различные ключи поэтому такие алгоритмы также называются ассиметричными.

Основным преимуществом таких алгоритмов является то, что один из участников схемы обмена данными (отправитель), не может его расшифровать. Таким образом имея зашифрованное сообщение, ключ с помощью которого сообщение шифровалось и зная алгоритм шифрования любой пользователь не имеет возможности расшифровать закодированное сообщение.

Ключ, с помощью которого один из участников схемы обмена сообщения (отправитель) шифрует исходное сообщение называется открытым и так как с его помощью невозможно расшифровать сообщение он может быть свободно опубликован. Другой ключ с применением которого дешифруется сообщение называется закрытым и должен быть известен только получателю зашифрованного сообщения.

Вся суть алгоритмов с открытым ключом заключается в использовании так называемых необратимых функций. Такие функции позволяют просто вычислить значение функции  $f(x)$ , но по известному значению функции  $y = f(x)$ , невозможно достоверно вычислить значение аргумента  $x$ .

В реальных условиях не любая необратимая функция может быть использована в криптосистемах. В криптографии в понятие необратимость вкладывается не теоретическая необратимость функции, а невозможность (в связи с высокой трудоемкостью) вычислить обратное значение функции используя современные мощные вычислительные системы за некоторый интервал времени, когда информация будет актуальна.

Для обеспечения гарантии защиты данных на криптосистемы с открытым ключом накладываются два важных требования:

- шифрование сообщения должно быть условно необратимым, а также исключить восстановление текста с использованием открытого ключа;
- вычисление закрытого ключа должно быть невозможным за определенный интервал времени с применением современных технических вычислительных систем.

Используемые сегодня криптосистемы с открытым ключом применяют одно из следующих необратимых преобразований:

- факторизация (разложение числа большой величины на простые множители), например алгоритм RSA;
- вычисление дискретного логарифма или дискретное возведение в степень в конечном поле;
- вычисление корней алгебраических уравнений.

### **Пример применения алгоритма RSA**

Хоть работа Диффи-Хеллмана и дала большой теоретический задел для криптосистем с открытым ключом, но первой реальной используемой подобной криптосистемой считается алгоритм RSA.

Криптографическая стойкость алгоритма RSA основывается на высокой вычислительной сложности процесса факторизации больших чисел (разложение на простые множители).

Безусловно факторизация чисел небольшой длины легко реализуема с использованием современных технических вычислительных систем, поэтому на практике используют ключи длина которых более 1024 бит.

Для упрощения вычислений в рассматриваемом примере будут применяться ключи меньшей длины.

Последовательность действий в алгоритме RSA следующая:

- 1) находим два простых числа  $p$  и  $q$ ;
- 2) вычисляем произведение  $n = p \cdot q$ ;
- 3) вычисляем функцию Эйлера  $\varphi(n) = (n - p)(q - 1)$ ;

4) выбираем открытый ключ  $e$  как произвольное число в диапазоне  $0 < e < n$  взаимно простое с функцией Эйлера;

5) вычисляем закрытый ключ  $d$  как обратное число по модулю  $\varphi(n)$  из отношения  $(d \cdot e) \bmod \varphi(n) = 1$ ;

6) пара  $\{e, n\}$  – это ключ, который открыто публикуется в месте где исключена возможность его фальсификации;

7) пара  $\{d, n\}$  – это ключ, который используется для дешифровки сообщения;

8) сообщение  $A$  шифруется по формуле  $S = A^e \bmod n$ , а дешифруется по формуле  $A = S^d \bmod n$ .

В качестве примера использовалось четверостишие стихотворения А. Блока:

Ночь, улица, фонарь, аптека,  
Бессмысленный и тусклый свет.  
Живи ещё хоть четверть века —  
Всё будет так. Исхода нет.

Алгоритм шифрования текстового сообщения, следующий:

1) применив таблицу замен (например ASCII, см. приложение Б), и получив соответствующие значения (Таблица 4.1);

2) так как в таблице ASCII кодов 255 символов, то находим два простых числа  $p$  и  $q$  такие что  $n = p \cdot q > 255$  тогда:  $p = 17$ ,  $q = 19$ ,  $n = 17 \cdot 19 = 323$ ;

3) тогда функция Эйлера  $\varphi(n) = 288$ ;

4) из условия  $0 < e < n$  выберем  $e = 11$ . Открыто публикуется пара  $\{11, 323\}$ ;

5) применив открытый ключ шифруем числа  $S = A^{11} \bmod 323$ , полученные в таблице 4.1 (Таблица 4.2);

6) из отношения  $(d \cdot 11) \bmod 288 = 1$  вычисляется  $d = 131$ , тогда пара  $\{131, 323\}$  это закрытый ключ;

7) применив закрытый ключ, дешифруем сообщение  
 $A = S^{131} \bmod 323$  (таблица 4.3);

8) применив таблицу ASCII, производим обратное преобразование из  
кода в символ (таблица 4.4);

Таблица 4.1 – Результаты замены символов на цифры

Символ	Н	о	ч	ь	,		у	л	и	ц	а	,		ф	о	н	а	р	ь	,		а	п	т	е	к	а	,	
Код символа	2	2	2	2	4	3	2	2	2	2	2	4	3	2	2	2	2	2	2	4	3	2	2	2	2	2	2	4	
Символ	Б	е	с	с	м	ы	с	л	е	н	н	ы	й		и		т	у	с	к	л	ы	й		с	в	е	т	.
Код символа	1	2	2	2	2	2	2	2	2	2	2	2	2	3	2	3	2	2	2	2	2	2	2	2	2	2	2	2	4
Символ	Ж	и	в	и		е	щ	ё		х	о	т	ь		ч	е	т	в	е	р	т	ь		в	е	к	а		—
Код символа	1	2	2	2	3	2	2	1	3	2	2	2	2	3	2	2	2	2	2	2	2	2	3	2	2	2	2	3	1
Символ	В	с	ё		б	у	д	е	т		т	а	к	.		И	с	х	о	д	а		н	е	т	.			
Код символа	1	2	1	3	2	2	2	2	2	3	2	2	2	4	3	2	2	2	2	2	2	3	2	2	2	4			

Таблица 4.2 – Зашифрованное сообщение

Код символа	2	2	2	2	4	3	2	2	2	2	2	4	3	2	2	2	2	2	2	4	3	2	2	2	2	2	4	
Зашифрованное сообщ.	3	2	3	4	2	2	7	1	3	1	4	2	2	2	2	4		4	2	2	4	2	2	1	1	5	4	2
Код символа	1	2	2	2	2	2	2	2	2	2	2	2	3	2	3	2	2	2	2	2	2	2	3	2	2	2	2	4

Зашифрованное сообщ.	1 2 4	1 7 2	2 1 1	2 1 1	1 4 5	2 2 5	2 1 1	1 6 3	1 7 2	2 7 1	2 7 1	2 2 5	6 0 0	2 3 1	2 3 0	1 3 0	7 9 1	2 1 1	5 5 3	1 6 3	2 2 5	6 0 0	2 3 1	2 2 2	2 3 2	1 7 2	1 3 0	2 7 8
Код символа	1 9 8	2 3 2	2 2 6	2 3 2	3 2 2	2 2 9	2 4 9	1 8 4	3 2 2	2 4 5	2 3 8	2 4 2	2 5 2	2 3 7	2 4 9	2 4 2	2 2 6	2 2 9	2 4 0	2 4 2	2 5 2	3 2 2	2 2 6	2 2 9	2 3 4	2 2 4	3 2 4	1 5 1
Зашифрованное сообщ.	1 2	3 0 1	2 3 2	3 0 1	2 3 0	1 7 2	1 4 8	7 8 0	2 3 0	9 9 4	2 0 4	1 3 4	4 4 0	2 3 0	1 7 2	1 3 2	2 3 2	1 7 2	8 0 0	1 3 4	4 4 0	2 3 2	2 3 2	1 7 2	5 5 5	4 1 0	2 3 0	9 4 4
Код символа	1 9 4	2 4 1	1 8 4	3 2 4	2 2 5	2 4 3	2 2 8	2 2 9	2 4 2	3 2 2	2 4 2	2 2 4	2 3 4	4 6 0	3 2 0	2 4 1	2 4 5	2 3 8	2 2 8	2 2 4	3 2 4	2 3 7	2 2 9	2 4 2	4 6 2			
Зашифрованное сообщ.	3 2 0	2 1 1	7 8 0	2 3 0	4 7 9	7 9 3	1 3 3	1 7 2	1 3 2	2 3 0	1 3 3	4 1 5	5 8 0	2 7 0	2 3 2	2 4 1	9 9 4	2 0 4	1 3 3	4 1 0	2 3 0	2 7 1	1 7 2	1 3 3	2 7 8			

Таблица 4.3 – Зашифрованное сообщение

Зашифрованное сообщ.	3 0 7	2 0 4	3 0 4	4 4 4	2 0 7	2 3 0	7 9 9	1 6 3	3 0 1	1 8 9	4 1 7	2 0 0	2 3 0	2 9 4	2 0 4	2 7 1	4 1 8	4 4 4	2 0 7	2 3 0	4 1 3	2 7 3	1 3 2	1 7 2	5 5 5	4 1 1	2 0 7		
Код символа	2 0 5	2 3 8	2 4 7	2 5 2	4 4 2	3 2 3	2 4 3	2 3 5	2 3 2	2 4 6	2 4 4	4 4 2	3 2 4	2 4 4	2 3 8	2 3 7	2 4 0	2 5 2	4 4 2	3 2 4	2 2 4	2 3 9	2 4 9	2 2 9	2 3 4	2 2 4	4 4 4		
Зашифрованное сообщ.	1 2 4	1 7 2	2 1 1	2 1 1	1 4 5	2 2 5	2 1 1	1 6 3	1 7 2	2 7 1	2 7 1	2 2 5	6 0 0	2 3 1	3 0 0	1 3 9	7 9 1	2 1 1	5 5 3	1 6 3	2 2 5	6 0 0	2 3 1	2 2 2	2 3 2	1 7 2	1 3 0	2 7 8	
Код символа	1 9 3	2 2 9	2 4 1	2 4 1	2 3 6	2 5 1	2 4 1	2 3 5	2 2 9	2 3 7	2 2 7	2 2 1	2 3 3	3 2 2	2 3 2	2 4 2	2 4 3	2 4 1	2 2 4	2 3 5	2 3 1	2 3 3	2 3 2	3 2 1	2 4 2	2 2 9	2 4 2	4 6 6	



Зашифрованное сообщ.	1 2	3 0 1	2 3 2	3 0 1	2 3 0	1 7 2	1 4 8	7 8	2 3 0	9 9	2 0 4	1 3 4	4 4	2 3 0	3 0 4	1 7 2	1 3 2	2 7 8	1 3 4	4 4	2 3 0	2 3 2	1 7 2	5 5	4 1	2 3 0	9 4
Код символа	1 9 8	2 3 2	2 2 6	2 3 2	3 2 2	2 2 9	2 4 9	1 8 4	3 2	2 4 5	2 3 8	2 4 2	2 5 2	3 2	2 4 7	2 2 9	2 4 0	2 2 0	2 4 2	2 4 2	3 2	2 2 6	2 2 9	2 3 4	2 2 4	3 2	1 5 1
Зашифрованное сообщ.	3 2 0	2 1 1	7 8	2 3 0	4 7	7 9	1 3 3	1 7 2	1 3	2 3 0	1 3 3	4 1 5	5 5	2 7 8	2 3 0	2 4 2	2 1 9	2 9 4	1 3 3	4 1 0	2 3 0	2 7 1	1 7 2	1 3	2 7 8		
Код символа	1 9 4	2 4 1	1 8 4	3 2	2 2 5	2 4 3	2 2 8	2 2 9	2 4 2	3 2	2 4 2	2 2 4	2 3 4	4 6	3 2	2 0	2 4 5	2 4 8	2 2 8	2 2 4	3 2	2 3 7	2 2 9	2 4 2	4 6		

Таблица 4.4 – Результаты замены кода на символы

Код символа	2 0 5	2 3 8	2 4 7	2 5 2	4 4	3 2	2 4 3	2 3 5	2 3 2	2 4 6	2 2 4	4 4	3 2	2 4 4	2 3 8	2 3 7	2 2 4	2 5 2	4 4	3 2	2 2 4	2 3 9	2 4 2	2 2 9	2 3 4	2 2 4	4 4		
Символ	Н	о	ч	ь	,		у	л	и	ц	а	,		ф	о	н	а	р	ь	,		а	п	т	е	к	а	,	
Код символа	1 9 3	2 2 9	2 4 1	2 4 1	2 3 6	2 5 1	2 4 1	2 3 5	2 2 9	2 3 7	2 3 7	2 5 1	3 3	2 2	2 3	2 4	2 4	2 4	2 3	2 4	2 3	2 5	2 3	2 3	2 4	2 2	2 2	4 6	
Символ	Б	е	с	с	м	ы	с	л	е	н	н	ы	й		и		т	у	с	к	л	ы	й		с	в	е	т	.
Код символа	1 9 8	2 3 2	2 2 6	2 3 2	3 2	2 2 9	2 4 9	1 8 4	3 2	2 4 5	2 3 8	2 4 2	2 5 2	3 2	2 4 7	2 2 9	2 4 2	2 2 6	2 4 9	2 4 0	2 2	2 3	2 2	2 3	2 2	2 3	3 2	1 5 1	
Символ	Ж	и	в	и		е	щ	ё		х	о	т	ь		ч	е	т	в	е	р	т	ь		в	е	к	а		—
Код символа	1 9 4	2 4 1	1 8 4	3 2	2 5	2 4 3	2 2 8	2 2 9	2 4 2	3 2	2 4 2	2 2 4	2 3 4	4 6	3 2	2 0	2 4 1	2 4 5	2 2 8	2 2 8	2 2	3 2	2 3	2 2	2 4	4 6			
Символ	В	с	ё		б	у	д	е	т		т	а	к	.		И	с	х	о	д	а		н	е	т	.			

## **Указания по технике безопасности**

В начале каждого семестра, со студентами должен проводиться инструктаж по технике безопасности в лаборатории. Во время нахождения студента в лаборатории и выполнения лабораторных работ студент не должен нарушать инструкции по охране труда с персональным компьютером ИОТ-37-ИВЛ-19, и инструкцию о мерах пожарной безопасности ИБП-01-2016.

## **Методические указания к выполнению работы**

Каждому студенту необходимо зашифровать и расшифровать текст полученный в первой работе.

При выполнении работы разрешается использовать любые технические и программные средства.

## **Содержание отчета**

- 1) Титульный лист (Пример в приложении В).
- 2) Цель работы.
- 3) Таблицы, вычисления, примеры расчетов.
- 4) Зашифрованный и расшифрованный текст.
- 5) Выводы.

## **Контрольные вопросы**

- 1) В чем заключается алгоритм RSA?
- 2) Для чего и почему используют комбинированные криптоалгоритмы?
- 3) В чем заключаются достоинства и недостатки асимметричных алгоритмов?
- 4) В чем заключаются достоинства и недостатки симметричных алгоритмов?

## **Литература**

- 1) Титов, А. А. Инженерно-техническая защита информации: учебное пособие / А. А. Титов. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL:

<http://www.iprbookshop.ru/13931.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

2) Литвинов, Р. В. Технические средства защиты информации. Часть 1: курс лекций / Р. В. Литвинов, К. А. Волегов, А. П. Бацула. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2006. — 170 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/14027.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

3) Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 95 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17925.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

4) Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 104 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17926.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

## **Тема 6. Методы защиты информации с применением методов основанных на разделении данных**

### **Лабораторная работа №5 «Изучение математических моделей схем порогового разделение данных, основанных на геометрических законах и численных методов их реализации»**

**Цель работы:** изучить математические модели порогового разделения данных и численные методы их реализации.

#### **Программа работы**

- 1) Изучить теоретический материал, математические и алгоритмические особенности схем порогового разделения данных.
- 2) В соответствии с заданием построить математическую модель алгоритма порогового разделения данных.

#### **Элементы теории**

В криптографии под термином разделение секрета понимается любой из способов распределения секрета среди группы участников каждому из которых достается только своя доля.

Такие схемы применяются в том случае, когда существует большая вероятность компрометации одного или нескольких участников, но вероятность предварительного сговора участников считается пренебрежимо малой.

Простейшим методом реализации подобной схемы является следующий пример:

пусть существует группа из  $n$  участников схемы разделения секрета и сообщение  $S$  длиной  $l$  состоящее из набора двоичных символов. Подбрав случайным образом набор двоичных сообщений  $S_1, S_2, S_3, \dots, S_n$  таких, что в сумме будут давать  $S$  и распространив среди всех участников схемы разделения секрета, то восстановить секрет будет возможно только в том случае, когда  $n$  участников соберутся вместе.

Пороговое разделение секрета отличается от процедуры разбиения тем, что для восстановления исходной информации потребуется только  $k$  из  $n$  исходных частей, на которые секрет был разделен.

Идею таких схемы независимо друг от друга предложили в 1979 г. Адди Шамир и Джордж Блэкли.

В таких схемах под понятием разрешенная коалицией понимают такое количество участников, которые имеют достаточное количество долей для восстановления секрета.

### **Концепция схемы разделения секрета Шамира**

Пороговая схема Шамира построена вокруг концепции полиномиальной интерполяции. Главная идея этой концепции состоит в том, что интерполяция невозможна если известно меньшее количество точек. Другими словами, через две точки на плоскости можно построить неограниченное количество кривых степени 2, и чтобы построить через из них единственно верную кривую нужна третья точка (рисунок 5.1).

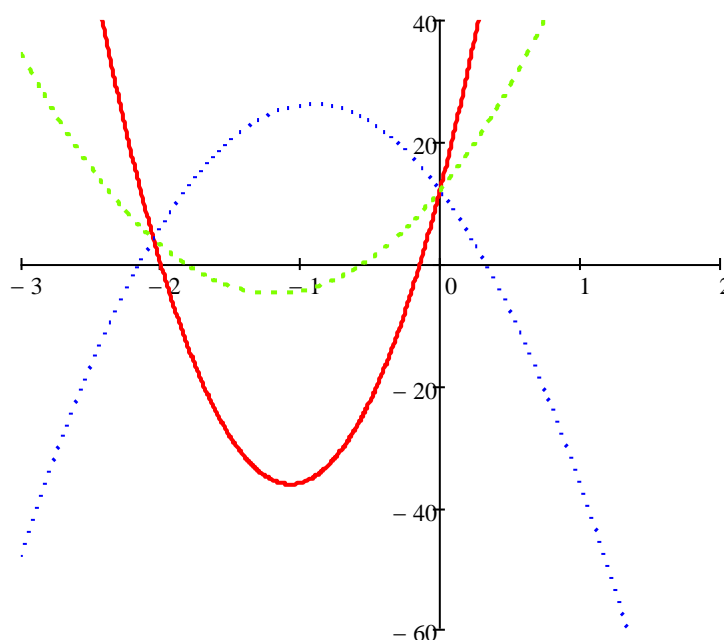


Рисунок 5.1 –Графическая иллюстрация схемы Шамира

Для разделения секрета между  $n$  пользователями таким образом чтобы восстановить информацию с помощью  $k$  частей, секрет подставляют в качестве свободного члена полинома  $k - 1$  степени.

Восстановить этот полином, а следовательно, и сам секрет можно только по  $k$  точкам.

### Пример реализации схемы Шамира

Пусть необходимо разделить секретную информацию  $S = 50$  применив  $(k, n)$  схему Шамира для  $k = 3$  и  $n = 5$ .

Далее строятся полином вида:

$$y(x_i) = ax_i^2 + bx_i + S$$

где:  $a$  и  $b$  – случайные числа, а  $S$  – разделяемая информация.

Тогда получим набор уравнений:

$$y(x_1) = 42x_1^2 + 90x_1 + 50$$

$$y(x_2) = 42x_2^2 + 90x_2 + 50$$

$$y(x_3) = 42x_3^2 + 90x_4 + 50$$

$$y(x_4) = 42x_4^2 + 90x_4 + 50$$

$$y(x_5) = 42x_5^2 + 90x_5 + 50$$

Следующим этапом для каждого уравнение необходимо случайным образом необходимо сгенерировать  $x_i$  такие что:  $x_i \neq x_{i+1} \neq x_{i+1} \neq \dots \neq x_n$ . Тогда примем  $x_1 = 9, x_2 = 18, x_3 = 27, x_4 = 4, x_5 = 87$ .

Подставив все значения получим следующие координаты: (9;4262); (18;15278); (27;33098); (4;1082); (87;325778) которые распределяются среди пользователей.

Используя формулу:

$$F(x) = \sum_{i=1}^k l_i(x)$$

строится интерполяционный полином Лагранжа.

где:

$$l_i = y(x_i) \prod_{\substack{j=1 \\ i \neq j}}^k \frac{x - x_j}{x_i - x_j}$$

Тогда при  $k = 3$  получим:

$$F(x) = y(x_1) \left( \frac{x - x_2}{x_1 - x_2} \cdot \frac{x - x_3}{x_1 - x_3} \right) + y(x_2) \left( \frac{x - x_1}{x_2 - x_1} \cdot \frac{x - x_3}{x_2 - x_3} \right) + y(x_3) \left( \frac{x - x_1}{x_3 - x_1} \cdot \frac{x - x_2}{x_3 - x_2} \right)$$

Подставив: (18; 15278); (27; 33098); (87; 325778) получим:

$$F(x) = 18 \left( \frac{x - 33098}{15278 - 33098} \cdot \frac{x - 325778}{15278 - 325778} \right) + 27 \left( \frac{x - 15278}{33098 - 15278} \cdot \frac{x - 325778}{33098 - 325778} \right) + 87 \left( \frac{x - 15278}{x_3 - 15278} \cdot \frac{x - 33098}{325778 - 33098} \right) = 42x^2 + 90x + 50.$$

Из получившегося уравнения  $S = F(0) = 42 \cdot 0^2 + 90 \cdot 0 + 50 = 50$ .

### **Концепция схемы разделения Блэкли**

Джордж Блэкли предложил свою схему, основанную на принципе векторного разделения секрета.

В такой схеме секретом является одна из координат  $k$ - мерной плоскости в  $k$ - мерном пространстве. Частями разделяемого секрета является уравнения  $k - 1$  – мерных гиперплоскостей.

Основная концепция схемы разделения секрета Блэкли заключается в следующем: пересечением  $k - 1$  линейно независимых уравнений плоскостей  $k - 1$  порядка является прямая; пересечением  $k$  линейно независимых плоскостей  $k - 1$  порядка является точка. Одна из координат пересечения  $k - 1$  мерных плоскостей в  $k$  – мерном пространстве и будет разделяемым секретом.

Схема Блэкли для  $k = 3$  представлена на рисунке 5.2.

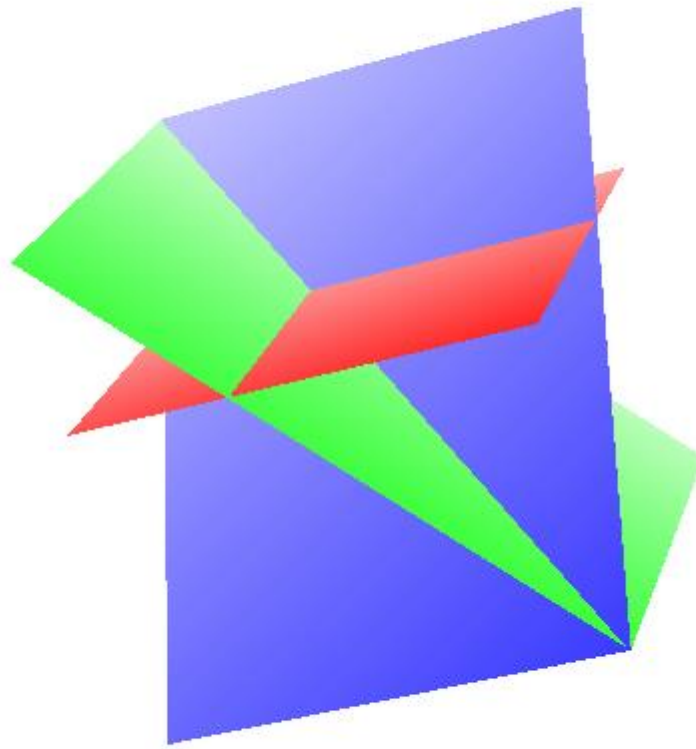


Рисунок 5.2 –Схема разделения секрета Блэкли

### Пример реализации схемы Блэкли

Пусть необходимо разделить секретную информацию  $S = 50$  применив  $(k, n)$  схему Блэкли для  $k = 3$  и  $n = 5$ . Для этого необходимо построить следующие уравнения:

$$\begin{cases} y_1 = a_{1,1} \cdot S + a_{1,2} \cdot x_{1,2} + \dots + a_{1,k} \cdot x_{1,k} \\ y_2 = a_{2,1} \cdot S + a_{2,2} \cdot x_{2,2} + \dots + a_{2,k} \cdot x_{2,k} \\ \dots \\ y_n = a_{n,1} \cdot S + a_{n,2} \cdot x_{n,2} + \dots + a_{n,k} \cdot x_{n,k} \end{cases}$$

Тогда получим:

$$\begin{cases} y_1 = 6 \cdot 50 + 5 \cdot x_{1,2} + 6 \cdot x_{1,3} \\ y_2 = 9 \cdot 50 + 3 \cdot x_{2,2} + 1 \cdot x_{2,3} \\ y_3 = 10 \cdot 50 + 6 \cdot x_{3,2} + 1 \cdot x_{3,3} \\ y_4 = 10 \cdot 50 + 8 \cdot x_{4,2} + 10 \cdot x_{4,3} \\ y_5 = 5 \cdot 50 + 1 \cdot x_{5,2} + 6 \cdot x_{5,3} \end{cases}$$

Причем любые  $k$  уравнений должны быть линейно независимы, то есть следующие уравнения должны образовывать базис:



$$- \begin{cases} y_1 = 6 \cdot 50 + 5 \cdot x_{1,2} + 6 \cdot x_{1,3} \\ y_2 = 9 \cdot 50 + 3 \cdot x_{2,2} + 1 \cdot x_{2,3} ; \\ y_3 = 10 \cdot 50 + 6 \cdot x_{3,2} + 1 \cdot x_{3,3} \end{cases}$$

$$- \begin{cases} y_1 = 6 \cdot 50 + 5 \cdot x_{1,2} + 6 \cdot x_{1,3} \\ y_2 = 9 \cdot 50 + 3 \cdot x_{2,2} + 1 \cdot x_{2,3} ; \\ y_4 = 10 \cdot 50 + 8 \cdot x_{4,2} + 10 \cdot x_{4,3} \end{cases}$$

$$- \begin{cases} y_1 = 6 \cdot 50 + 5 \cdot x_{1,2} + 6 \cdot x_{1,3} \\ y_2 = 9 \cdot 50 + 3 \cdot x_{2,2} + 1 \cdot x_{2,3}; \\ y_5 = 5 \cdot 50 + 1 \cdot x_{5,2} + 6 \cdot x_{5,3} \end{cases}$$

$$- \begin{cases} y_1 = 6 \cdot 50 + 5 \cdot x_{1,2} + 6 \cdot x_{1,3} \\ y_3 = 10 \cdot 50 + 6 \cdot x_{3,2} + 1 \cdot x_{3,3} ; \\ y_4 = 10 \cdot 50 + 8 \cdot x_{4,2} + 10 \cdot x_{4,3} \end{cases}$$

$$- \begin{cases} y_1 = 6 \cdot 50 + 5 \cdot x_{1,2} + 6 \cdot x_{1,3} \\ y_3 = 10 \cdot 50 + 6 \cdot x_{3,2} + 1 \cdot x_{3,3}; \\ y_5 = 5 \cdot 50 + 1 \cdot x_{5,2} + 6 \cdot x_{5,3} \end{cases}$$

$$- \begin{cases} y_2 = 9 \cdot 50 + 3 \cdot x_{2,2} + 1 \cdot x_{2,3} \\ y_3 = 10 \cdot 50 + 6 \cdot x_{3,2} + 1 \cdot x_{3,3} ; \\ y_4 = 10 \cdot 50 + 8 \cdot x_{4,2} + 10 \cdot x_{4,3} \end{cases}$$

$$- \begin{cases} y_2 = 9 \cdot 50 + 3 \cdot x_{2,2} + 1 \cdot x_{2,3} \\ y_3 = 10 \cdot 50 + 6 \cdot x_{3,2} + 1 \cdot x_{3,3}; \\ y_5 = 5 \cdot 50 + 1 \cdot x_{5,2} + 6 \cdot x_{5,3} \end{cases}$$

$$- \begin{cases} y_2 = 9 \cdot 50 + 3 \cdot x_{2,2} + 1 \cdot x_{2,3} \\ y_4 = 10 \cdot 50 + 8 \cdot x_{4,2} + 10 \cdot x_{4,3}; \\ y_5 = 5 \cdot 50 + 1 \cdot x_{5,2} + 6 \cdot x_{5,3} \end{cases}$$

$$- \begin{cases} y_3 = 10 \cdot 50 + 6 \cdot x_{3,2} + 1 \cdot x_{3,3} \\ y_4 = 10 \cdot 50 + 8 \cdot x_{4,2} + 10 \cdot x_{4,3}. \\ y_5 = 5 \cdot 50 + 1 \cdot x_{5,2} + 6 \cdot x_{5,3} \end{cases}$$

Зная  $n$  уравнений, необходимо выбрать числа  $x_{1,*} = 2$  и  $x_{2,*} = 5$  и подставить. Тогда получим:

$$\begin{cases} y_1 = 6 \cdot 50 + 5 \cdot 2 + 6 \cdot 5 = 340 \\ y_2 = 9 \cdot 50 + 3 \cdot 2 + 1 \cdot 5 = 461 \\ y_3 = 10 \cdot 50 + 6 \cdot 2 + 1 \cdot 5 = 517 \\ y_4 = 10 \cdot 50 + 8 \cdot 2 + 10 \cdot 5 = 566 \\ y_5 = 5 \cdot 50 + 1 \cdot 2 + 6 \cdot 5 = 282 \end{cases}$$

Каждому участнику раздаются следующие коэффициенты: {6,5,6,340}; {9,3,1,461}; {10,6,1,517}; {10,8,10,566}; {5,1,6,282}.

Теперь восстановить секрет можно имея  $k = 3$  частей секрета.

Для восстановления секрета используем следующие части: {5,5,6,440}; {9,3,1,461}; {5,1,6,282}. Для этого необходимо составить систему уравнений:

$$\begin{cases} 6x_1 + 5x_2 + 6x_3 = 340 \\ 9x_1 + 3x_2 + 1x_3 = 461 \\ 5x_1 + 1x_2 + 6x_3 = 282 \end{cases}$$

Для нахождения секрета необходимо решить эту систему уравнений для чего можно применить: метод Крамера; матричный метод; метод Гаусса; либо любой другой доступный и удобный способ. Решив систему уравнений методом Гаусса, получим:

$$\left( \begin{array}{ccc|c} 1 & 0 & 0 & 50 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 5 \end{array} \right)$$

Следовательно координаты точки будет следующие: (50; 2; 5). Так как секрет подставляли в координату первого коэффициента уравнения, следовательно секрет  $S = 50$ .

### **Указания по технике безопасности**

В начале каждого семестра, студентам должен проводиться инструктаж по технике безопасности в лаборатории. Во время нахождения студента в лаборатории и выполнения лабораторных работ студент должен соблюдать инструкцию по охране труда с персональным компьютером ИОТ-37-ИВЛ-19, и инструкцию о мерах пожарной безопасности ИБП-01-2016.

### **Методические указания к выполнению работы**

Каждому студенту задается разделенное слово с применением  $(k, n)$  пороговых схем разделения секрета Шамира и Блэкли при  $k = 3$  и  $n = 5$ . Слово предварительно закодировано с применением таблицы ASCII кодов (Приложение Б). Необходимо в соответствии с вариантом восстановить слово, разделенное этими алгоритмами. Важно восстановить при  $k = 3$  и  $k = 5$ .

При выполнении работы разрешается использовать любые технические и программные средства.

Таблица 5.1 – Задания для выполнения работы

Вариант	Задание					
1)	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{3; 576}	{3; 588}	{3; 591}	{3; 595}	{3; 587}	{3; 576}
	{4; 828}	{4; 840}	{4; 843}	{4; 847}	{4; 839}	{4; 828}
	{5; 1142}	{5; 1154}	{5; 1157}	{5; 1161}	{5; 1153}	{5; 1142}
	{9; 3018}	{9; 3030}	{9; 3033}	{9; 3037}	{9; 3029}	{9; 3018}
	{12; 5076}	{12; 5088}	{12; 5091}	{12; 5095}	{12; 5087}	{12; 5076}
	Схема Блэкли					
	X1	X2	X3	X4	X5	X6
	{3, 20, 12, 880}	{3, 20, 12, 916}	{3, 20, 12, 925}	{3, 20, 12, 937}	{3, 20, 12, 913}	{3, 20, 12, 880}
	{24, 2, 17, 4828}	{24, 2, 17, 5116}	{24, 2, 17, 5188}	{24, 2, 17, 5284}	{24, 2, 17, 5092}	{24, 2, 17, 4828}
	{7, 6, 27, 1716}	{7, 6, 27, 1800}	{7, 6, 27, 1821}	{7, 6, 27, 1849}	{7, 6, 27, 1793}	{7, 6, 27, 1716}
	{23, 18, 30, 4920}	{23, 18, 30, 5196}	{23, 18, 30, 5265}	{23, 18, 30, 5357}	{23, 18, 30, 5173}	{23, 18, 30, 4920}
{10, 9, 15, 2172}	{10, 9, 15, 2292}	{10, 9, 15, 2322}	{10, 9, 15, 2362}	{10, 9, 15, 2282}	{10, 9, 15, 2172}	
2)	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{1; 228}	{1; 241}	{1; 228}	{1; 239}	{1; 236}	{1; 235}
	{7; 948}	{7; 961}	{7; 948}	{7; 959}	{7; 956}	{7; 955}
	{8; 1152}	{8; 1165}	{8; 1152}	{8; 1163}	{8; 1160}	{8; 1159}
	{13; 2532}	{13; 2545}	{13; 2532}	{13; 2543}	{13; 2540}	{13; 2539}
	{15; 3252}	{15; 3265}	{15; 3252}	{15; 3263}	{15; 3260}	{15; 3259}
	Схема Блэкли					
	X1	X2	X3	X4	X5	X6
	{15, 21, 21, 3195}	{15, 21, 21, 3390}	{15, 21, 21, 3195}	{15, 21, 21, 3360}	{15, 21, 21, 3315}	{15, 21, 21, 3300}
	{17, 20, 30, 3634}	{17, 20, 30, 3855}	{17, 20, 30, 3634}	{17, 20, 30, 3821}	{17, 20, 30, 3770}	{17, 20, 30, 3753}
	{24, 19, 27, 4949}	{24, 19, 27, 5261}	{24, 19, 27, 4949}	{24, 19, 27, 5213}	{24, 19, 27, 5141}	{24, 19, 27, 5117}
	{30, 8, 29, 6027}	{30, 8, 29, 6417}	{30, 8, 29, 6027}	{30, 8, 29, 6357}	{30, 8, 29, 6267}	{30, 8, 29, 6237}

	{7, 21, 23, 1673}	{7, 21, 23, 1764}	{7, 21, 23, 1673}	{7, 21, 23, 1750}	{7, 21, 23, 1729}	{7, 21, 23, 1722}
3)	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{1; 203}	{1; 202}	{1; 213}	{1; 202}	{1; 215}	{1; 219}
	{2; 219}	{2; 218}	{2; 229}	{2; 218}	{2; 231}	{2; 235}
	{4; 269}	{4; 268}	{4; 279}	{4; 268}	{4; 281}	{4; 285}
	{9; 499}	{9; 498}	{9; 509}	{9; 498}	{9; 511}	{9; 515}
	{10; 563}	{10; 562}	{10; 573}	{10; 562}	{10; 575}	{10; 579}
	Схема Блэкли					
	X1	X2	X3	X4	X5	X6
	{8, 20, 22, 1756}	{8, 20, 22, 1748}	{8, 20, 22, 1836}	{8, 20, 22, 1748}	{8, 20, 22, 1852}	{8, 20, 22, 1884}
	{18, 16, 29, 3712}	{18, 16, 29, 3694}	{18, 16, 29, 3892}	{18, 16, 29, 3694}	{18, 16, 29, 3928}	{18, 16, 29, 4000}
	{19, 14, 14, 3807}	{19, 14, 14, 3788}	{19, 14, 14, 3997}	{19, 14, 14, 3788}	{19, 14, 14, 4035}	{19, 14, 14, 4111}
	{23, 30, 21, 4685}	{23, 30, 21, 4662}	{23, 30, 21, 4915}	{23, 30, 21, 4662}	{23, 30, 21, 4961}	{23, 30, 21, 5053}
{24, 17, 28, 4868}	{24, 17, 28, 4844}	{24, 17, 28, 5108}	{24, 17, 28, 4844}	{24, 17, 28, 5156}	{24, 17, 28, 5252}	
4)	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{2; 217}	{2; 216}	{2; 232}	{2; 217}	{2; 230}	{2; 233}
	{4; 257}	{4; 256}	{4; 272}	{4; 257}	{4; 270}	{4; 273}
	{6; 313}	{6; 312}	{6; 328}	{6; 313}	{6; 326}	{6; 329}
	{7; 347}	{7; 346}	{7; 362}	{7; 347}	{7; 360}	{7; 363}
	{8; 385}	{8; 384}	{8; 400}	{8; 385}	{8; 398}	{8; 401}
	Схема Блэкли					
	X1	X2	X3	X4	X5	X6
	{2, 28, 12, 678}	{2, 28, 12, 676}	{2, 28, 12, 708}	{2, 28, 12, 678}	{2, 28, 12, 704}	{2, 28, 12, 710}
	{9, 13, 21, 1996}	{9, 13, 21, 1987}	{9, 13, 21, 2131}	{9, 13, 21, 1996}	{9, 13, 21, 2113}	{9, 13, 21, 2140}
	{29, 16, 16, 5837}	{29, 16, 16, 5808}	{29, 16, 16, 6272}	{29, 16, 16, 5837}	{29, 16, 16, 6214}	{29, 16, 16, 6301}
	{26, 25, 17, 5329}	{26, 25, 17, 5303}	{26, 25, 17, 5719}	{26, 25, 17, 5329}	{26, 25, 17, 5667}	{26, 25, 17, 5745}
{16, 1, 20, 3255}	{16, 1, 20, 3239}	{16, 1, 20, 3495}	{16, 1, 20, 3255}	{16, 1, 20, 3463}	{16, 1, 20, 3511}	
5)	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{1; 204}	{1; 202}	{1; 213}	{1; 232}	{1; 220}	{1; 202}
	{2; 218}	{2; 216}	{2; 227}	{2; 246}	{2; 234}	{2; 216}
	{9; 428}	{9; 426}	{9; 437}	{9; 456}	{9; 444}	{9; 426}
	{12; 578}	{12; 576}	{12; 587}	{12; 606}	{12; 594}	{12; 576}
	{15; 764}	{15; 762}	{15; 773}	{15; 792}	{15; 780}	{15; 762}

Схема Блэкли					
X1	X2	X3	X4	X5	X6
{18, 9, 6, 3600}	{18, 9, 6, 3564}	{18, 9, 6, 3762}	{18, 9, 6, 4104}	{18, 9, 6, 3888}	{18, 9, 6, 3564}
{7, 6, 20, 1574}	{7, 6, 20, 1560}	{7, 6, 20, 1637}	{7, 6, 20, 1770}	{7, 6, 20, 1686}	{7, 6, 20, 1560}
{5, 16, 19, 1237}	{5, 16, 19, 1227}	{5, 16, 19, 1282}	{5, 16, 19, 1377}	{5, 16, 19, 1317}	{5, 16, 19, 1227}
{13, 13, 5, 2645}	{13, 13, 5, 2619}	{13, 13, 5, 2762}	{13, 13, 5, 3009}	{13, 13, 5, 2853}	{13, 13, 5, 2619}
{17, 2, 17, 3463}	{17, 2, 17, 3429}	{17, 2, 17, 3616}	{17, 2, 17, 3939}	{17, 2, 17, 3735}	{17, 2, 17, 3429}

Схема Шамира					
X1	X2	X3	X4	X5	X6
{1; 209}	{1; 212}	{1; 225}	{1; 228}	{1; 215}	{1; 216}
{2; 230}	{2; 233}	{2; 246}	{2; 249}	{2; 236}	{2; 237}
{9; 545}	{9; 548}	{9; 561}	{9; 564}	{9; 551}	{9; 552}
{12; 770}	{12; 773}	{12; 786}	{12; 789}	{12; 776}	{12; 777}
{15; 1049}	{15; 1052}	{15; 1065}	{15; 1068}	{15; 1055}	{15; 1056}

Схема Блэкли					
X1	X2	X3	X4	X5	X6
{18, 9, 6, 3600}	{18, 9, 6, 3654}	{18, 9, 6, 3888}	{18, 9, 6, 3942}	{18, 9, 6, 3708}	{18, 9, 6, 3726}
{7, 6, 20, 1574}	{7, 6, 20, 1595}	{7, 6, 20, 1686}	{7, 6, 20, 1707}	{7, 6, 20, 1616}	{7, 6, 20, 1623}
{5, 16, 19, 1237}	{5, 16, 19, 1252}	{5, 16, 19, 1317}	{5, 16, 19, 1332}	{5, 16, 19, 1267}	{5, 16, 19, 1272}
{13, 13, 5, 2645}	{13, 13, 5, 2684}	{13, 13, 5, 2853}	{13, 13, 5, 2892}	{13, 13, 5, 2723}	{13, 13, 5, 2736}
{17, 2, 17, 3463}	{17, 2, 17, 3514}	{17, 2, 17, 3735}	{17, 2, 17, 3786}	{17, 2, 17, 3565}	{17, 2, 17, 3582}

Схема Шамира					
X1	X2	X3	X4	X5	X6
{2; 203}	{2; 200}	{2; 202}	{2; 200}	{2; 213}	{2; 228}
{4; 219}	{4; 216}	{4; 218}	{4; 216}	{4; 229}	{4; 244}
{6; 243}	{6; 240}	{6; 242}	{6; 240}	{6; 253}	{6; 268}
{8; 275}	{8; 272}	{8; 274}	{8; 272}	{8; 285}	{8; 300}
{14; 419}	{14; 416}	{14; 418}	{14; 416}	{14; 429}	{14; 444}

Схема Блэкли					
X1	X2	X3	X4	X5	X6
{2, 29, 12, 455}	{2, 29, 12, 449}	{2, 29, 12, 453}	{2, 29, 12, 449}	{2, 29, 12, 475}	{2, 29, 12, 505}
{29, 8, 1, 5666}	{29, 8, 1, 5579}	{29, 8, 1, 5637}	{29, 8, 1, 5579}	{29, 8, 1, 5956}	{29, 8, 1, 6391}
{24, 1, 9, 4708}	{24, 1, 9, 4636}	{24, 1, 9, 4684}	{24, 1, 9, 4636}	{24, 1, 9, 4948}	{24, 1, 9, 5308}

	{29, 23, 8, 5702}	{29, 23, 8, 5615}	{29, 23, 8, 5673}	{29, 23, 8, 5615}	{29, 23, 8, 5992}	{29, 23, 8, 6427}
	{27, 10, 8, 5299}	{27, 10, 8, 5218}	{27, 10, 8, 5272}	{27, 10, 8, 5218}	{27, 10, 8, 5569}	{27, 10, 8, 5974}
8)	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{1; 208}	{1; 205}	{1; 212}	{1; 210}	{1; 216}	{1; 233}
	{2; 229}	{2; 226}	{2; 233}	{2; 231}	{2; 237}	{2; 254}
	{3; 258}	{3; 255}	{3; 262}	{3; 260}	{3; 266}	{3; 283}
	{5; 340}	{5; 337}	{5; 344}	{5; 342}	{5; 348}	{5; 365}
	{8; 523}	{8; 520}	{8; 527}	{8; 525}	{8; 531}	{8; 548}
	Схема Блэкли					
	X1	X2	X3	X4	X5	X6
	{5, 25, 20, 1255}	{5, 25, 20, 1240}	{5, 25, 20, 1275}	{5, 25, 20, 1265}	{5, 25, 20, 1295}	{5, 25, 20, 1380}
	{30, 28, 17, 6115}	{30, 28, 17, 6025}	{30, 28, 17, 6235}	{30, 28, 17, 6175}	{30, 28, 17, 6355}	{30, 28, 17, 6865}
	{23, 15, 17, 4698}	{23, 15, 17, 4629}	{23, 15, 17, 4790}	{23, 15, 17, 4744}	{23, 15, 17, 4882}	{23, 15, 17, 5273}
	{30, 16, 5, 5959}	{30, 16, 5, 5869}	{30, 16, 5, 6079}	{30, 16, 5, 6019}	{30, 16, 5, 6199}	{30, 16, 5, 6709}
	{28, 11, 19, 5675}	{28, 11, 19, 5591}	{28, 11, 19, 5787}	{28, 11, 19, 5731}	{28, 11, 19, 5899}	{28, 11, 19, 6375}
9)	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{2; 226}	{2; 222}	{2; 240}	{2; 245}	{2; 230}	{2; 232}
	{4; 272}	{4; 268}	{4; 286}	{4; 291}	{4; 276}	{4; 278}
	{7; 371}	{7; 367}	{7; 385}	{7; 390}	{7; 375}	{7; 377}
	{9; 457}	{9; 453}	{9; 471}	{9; 476}	{9; 461}	{9; 463}
	{12; 616}	{12; 612}	{12; 630}	{12; 635}	{12; 620}	{12; 622}
	Схема Блэкли					
	X1	X2	X3	X4	X5	X6
	{6, 12, 11, 1233}	{6, 12, 11, 1209}	{6, 12, 11, 1317}	{6, 12, 11, 1347}	{6, 12, 11, 1257}	{6, 12, 11, 1269}
	{9, 21, 17, 1857}	{9, 21, 17, 1821}	{9, 21, 17, 1983}	{9, 21, 17, 2028}	{9, 21, 17, 1893}	{9, 21, 17, 1911}
	{21, 3, 1, 4125}	{21, 3, 1, 4041}	{21, 3, 1, 4419}	{21, 3, 1, 4524}	{21, 3, 1, 4209}	{21, 3, 1, 4251}
	{27, 15, 18, 5376}	{27, 15, 18, 5268}	{27, 15, 18, 5754}	{27, 15, 18, 5889}	{27, 15, 18, 5484}	{27, 15, 18, 5538}
	{17, 11, 11, 3387}	{17, 11, 11, 3319}	{17, 11, 11, 3625}	{17, 11, 11, 3710}	{17, 11, 11, 3455}	{17, 11, 11, 3489}
10)	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{2; 214}	{2; 212}	{2; 224}	{2; 219}	{2; 220}	{2; 210}
	{4; 248}	{4; 246}	{4; 258}	{4; 253}	{4; 254}	{4; 244}
	{7; 329}	{7; 327}	{7; 339}	{7; 334}	{7; 335}	{7; 325}

	{9; 403}	{9; 401}	{9; 413}	{9; 408}	{9; 409}	{9; 399}
	{12; 544}	{12; 542}	{12; 554}	{12; 549}	{12; 550}	{12; 540}
	Схема Блэкли					
	X1	X2	X3	X4	X5	X6
	{19, 22, 24, 4074}	{19, 22, 24, 4036}	{19, 22, 24, 4264}	{19, 22, 24, 4169}	{19, 22, 24, 4188}	{19, 22, 24, 3998}
	{23, 9, 6, 4613}	{23, 9, 6, 4567}	{23, 9, 6, 4843}	{23, 9, 6, 4728}	{23, 9, 6, 4751}	{23, 9, 6, 4521}
	{18, 14, 30, 3898}	{18, 14, 30, 3862}	{18, 14, 30, 4078}	{18, 14, 30, 3988}	{18, 14, 30, 4006}	{18, 14, 30, 3826}
	{21, 2, 9, 4216}	{21, 2, 9, 4174}	{21, 2, 9, 4426}	{21, 2, 9, 4321}	{21, 2, 9, 4342}	{21, 2, 9, 4132}
	{8, 15, 27, 1913}	{8, 15, 27, 1897}	{8, 15, 27, 1993}	{8, 15, 27, 1953}	{8, 15, 27, 1961}	{8, 15, 27, 1881}
	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{2; 235}	{2; 251}	{2; 238}	{2; 234}	{2; 243}	{2; 230}
	{5; 367}	{5; 383}	{5; 370}	{5; 366}	{5; 375}	{5; 362}
	{6; 431}	{6; 447}	{6; 434}	{6; 430}	{6; 439}	{6; 426}
	{8; 589}	{8; 605}	{8; 592}	{8; 588}	{8; 597}	{8; 584}
	{13; 1159}	{13; 1175}	{13; 1162}	{13; 1158}	{13; 1167}	{13; 1154}
	Схема Блэкли					
11)	X1	X2	X3	X4	X5	X6
	{7, 23, 1, 1502}	{7, 23, 1, 1614}	{7, 23, 1, 1523}	{7, 23, 1, 1495}	{7, 23, 1, 1558}	{7, 23, 1, 1467}
	{27, 8, 15, 5479}	{27, 8, 15, 5911}	{27, 8, 15, 5560}	{27, 8, 15, 5452}	{27, 8, 15, 5695}	{27, 8, 15, 5344}
	{25, 10, 13, 5079}	{25, 10, 13, 5479}	{25, 10, 13, 5154}	{25, 10, 13, 5054}	{25, 10, 13, 5279}	{25, 10, 13, 4954}
	{1, 21, 30, 542}	{1, 21, 30, 558}	{1, 21, 30, 545}	{1, 21, 30, 541}	{1, 21, 30, 550}	{1, 21, 30, 537}
	{16, 3, 28, 3391}	{16, 3, 28, 3647}	{16, 3, 28, 3439}	{16, 3, 28, 3375}	{16, 3, 28, 3519}	{16, 3, 28, 3311}
	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{2; 217}	{2; 216}	{2; 220}	{2; 225}	{2; 239}	{2; 221}
	{5; 277}	{5; 276}	{5; 280}	{5; 285}	{5; 299}	{5; 281}
	{6; 305}	{6; 304}	{6; 308}	{6; 313}	{6; 327}	{6; 309}
	{8; 373}	{8; 372}	{8; 376}	{8; 381}	{8; 395}	{8; 377}
	{13; 613}	{13; 612}	{13; 616}	{13; 621}	{13; 635}	{13; 617}
	Схема Блэкли					
	X1	X2	X3	X4	X5	X6
	{14, 12, 26, 2938}	{14, 12, 26, 2924}	{14, 12, 26, 2980}	{14, 12, 26, 3050}	{14, 12, 26, 3246}	{14, 12, 26, 2994}
	{16, 20, 25, 3342}	{16, 20, 25, 3326}	{16, 20, 25, 3390}	{16, 20, 25, 3470}	{16, 20, 25, 3694}	{16, 20, 25, 3406}
	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{14, 12, 26, 2938}	{14, 12, 26, 2924}	{14, 12, 26, 2980}	{14, 12, 26, 3050}	{14, 12, 26, 3246}	{14, 12, 26, 2994}
	{16, 20, 25, 3342}	{16, 20, 25, 3326}	{16, 20, 25, 3390}	{16, 20, 25, 3470}	{16, 20, 25, 3694}	{16, 20, 25, 3406}

	{3, 16, 4, 647}	{3, 16, 4, 644}	{3, 16, 4, 656}	{3, 16, 4, 671}	{3, 16, 4, 713}	{3, 16, 4, 659}
	{11, 24, 16, 2311}	{11, 24, 16, 2300}	{11, 24, 16, 2344}	{11, 24, 16, 2399}	{11, 24, 16, 2553}	{11, 24, 16, 2355}
	{21, 28, 29, 4367}	{21, 28, 29, 4346}	{21, 28, 29, 4430}	{21, 28, 29, 4535}	{21, 28, 29, 4829}	{21, 28, 29, 4451}
13)	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{1; 213}	{1; 206}	{1; 212}	{1; 211}	{1; 229}	{1; 234}
	{2; 237}	{2; 230}	{2; 236}	{2; 235}	{2; 253}	{2; 258}
	{3; 271}	{3; 264}	{3; 270}	{3; 269}	{3; 287}	{3; 292}
	{11; 903}	{11; 896}	{11; 902}	{11; 901}	{11; 919}	{11; 924}
	{14; 1305}	{14; 1298}	{14; 1304}	{14; 1303}	{14; 1321}	{14; 1326}
	Схема Блэкли					
	X1	X2	X3	X4	X5	X6
	{3, 15, 7, 808}	{3, 15, 7, 787}	{3, 15, 7, 805}	{3, 15, 7, 802}	{3, 15, 7, 856}	{3, 15, 7, 871}
	{21, 9, 3, 4290}	{21, 9, 3, 4143}	{21, 9, 3, 4269}	{21, 9, 3, 4248}	{21, 9, 3, 4626}	{21, 9, 3, 4731}
	{29, 9, 8, 5947}	{29, 9, 8, 5744}	{29, 9, 8, 5918}	{29, 9, 8, 5889}	{29, 9, 8, 6411}	{29, 9, 8, 6556}
	{5, 12, 1, 1104}	{5, 12, 1, 1069}	{5, 12, 1, 1099}	{5, 12, 1, 1094}	{5, 12, 1, 1184}	{5, 12, 1, 1209}
{16, 18, 16, 3536}	{16, 18, 16, 3424}	{16, 18, 16, 3520}	{16, 18, 16, 3504}	{16, 18, 16, 3792}	{16, 18, 16, 3872}	
14)	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{4; 324}	{4; 323}	{4; 342}	{4; 347}	{4; 334}	{4; 344}
	{8; 608}	{8; 607}	{8; 626}	{8; 631}	{8; 618}	{8; 628}
	{9; 704}	{9; 703}	{9; 722}	{9; 727}	{9; 714}	{9; 724}
	{11; 926}	{11; 925}	{11; 944}	{11; 949}	{11; 936}	{11; 946}
	{15; 1490}	{15; 1489}	{15; 1508}	{15; 1513}	{15; 1500}	{15; 1510}
	Схема Блэкли					
	X1	X2	X3	X4	X5	X6
	{13, 4, 26, 2906}	{13, 4, 26, 2893}	{13, 4, 26, 3140}	{13, 4, 26, 3205}	{13, 4, 26, 3036}	{13, 4, 26, 3166}
	{8, 2, 11, 1731}	{8, 2, 11, 1723}	{8, 2, 11, 1875}	{8, 2, 11, 1915}	{8, 2, 11, 1811}	{8, 2, 11, 1891}
	{13, 6, 8, 2718}	{13, 6, 8, 2705}	{13, 6, 8, 2952}	{13, 6, 8, 3017}	{13, 6, 8, 2848}	{13, 6, 8, 2978}
	{21, 4, 17, 4407}	{21, 4, 17, 4386}	{21, 4, 17, 4785}	{21, 4, 17, 4890}	{21, 4, 17, 4617}	{21, 4, 17, 4827}
{14, 11, 20, 3075}	{14, 11, 20, 3061}	{14, 11, 20, 3327}	{14, 11, 20, 3397}	{14, 11, 20, 3215}	{14, 11, 20, 3355}	
15)	Схема Шамира					
	X1	X2	X3	X4	X5	X6



	{2; 252}	{2; 242}	{2; 253}	{2; 270}	{2; 252}	{2; 242}
	{8; 738}	{8; 728}	{8; 739}	{8; 756}	{8; 738}	{8; 728}
	{9; 868}	{9; 858}	{9; 869}	{9; 886}	{9; 868}	{9; 858}
	{11; 1170}	{11; 1160}	{11; 1171}	{11; 1188}	{11; 1170}	{11; 1160}
	{15; 1942}	{15; 1932}	{15; 1943}	{15; 1960}	{15; 1942}	{15; 1932}
	Схема Блэкли					
	X1	X2	X3	X4	X5	X6
	{14, 9, 29, 3210}	{14, 9, 29, 3070}	{14, 9, 29, 3224}	{14, 9, 29, 3462}	{14, 9, 29, 3210}	{14, 9, 29, 3070}
	{5, 19, 10, 1253}	{5, 19, 10, 1203}	{5, 19, 10, 1258}	{5, 19, 10, 1343}	{5, 19, 10, 1253}	{5, 19, 10, 1203}
	{26, 21, 23, 5652}	{26, 21, 23, 5392}	{26, 21, 23, 5678}	{26, 21, 23, 6120}	{26, 21, 23, 5652}	{26, 21, 23, 5392}
	{3, 26, 12, 920}	{3, 26, 12, 890}	{3, 26, 12, 923}	{3, 26, 12, 974}	{3, 26, 12, 920}	{3, 26, 12, 890}
	{11, 10, 17, 2479}	{11, 10, 17, 2369}	{11, 10, 17, 2490}	{11, 10, 17, 2677}	{11, 10, 17, 2479}	{11, 10, 17, 2369}
	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{1; 217}	{1; 207}	{1; 220}	{1; 207}	{1; 209}	{1; 207}
	{3; 289}	{3; 279}	{3; 292}	{3; 279}	{3; 281}	{3; 279}
	{9; 841}	{9; 831}	{9; 844}	{9; 831}	{9; 833}	{9; 831}
	{12; 1306}	{12; 1296}	{12; 1309}	{12; 1296}	{12; 1298}	{12; 1296}
	{14; 1686}	{14; 1676}	{14; 1689}	{14; 1676}	{14; 1678}	{14; 1676}
	Схема Блэкли					
16)	X1	X2	X3	X4	X5	X6
	{30, 8, 17, 6252}	{30, 8, 17, 5952}	{30, 8, 17, 6342}	{30, 8, 17, 5952}	{30, 8, 17, 6012}	{30, 8, 17, 5952}
	{14, 4, 12, 2952}	{14, 4, 12, 2812}	{14, 4, 12, 2994}	{14, 4, 12, 2812}	{14, 4, 12, 2840}	{14, 4, 12, 2812}
	{8, 15, 10, 1801}	{8, 15, 10, 1721}	{8, 15, 10, 1825}	{8, 15, 10, 1721}	{8, 15, 10, 1737}	{8, 15, 10, 1721}
	{30, 10, 9, 6202}	{30, 10, 9, 5902}	{30, 10, 9, 6292}	{30, 10, 9, 5902}	{30, 10, 9, 5962}	{30, 10, 9, 5902}
	{3, 23, 3, 791}	{3, 23, 3, 761}	{3, 23, 3, 800}	{3, 23, 3, 761}	{3, 23, 3, 767}	{3, 23, 3, 761}
	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{1; 216}	{1; 205}	{1; 218}	{1; 209}	{1; 232}	{1; 229}
	{3; 266}	{3; 255}	{3; 268}	{3; 259}	{3; 282}	{3; 279}
	{8; 531}	{8; 520}	{8; 533}	{8; 524}	{8; 547}	{8; 544}
17)	{10; 693}	{10; 682}	{10; 695}	{10; 686}	{10; 709}	{10; 706}
	{11; 786}	{11; 775}	{11; 788}	{11; 779}	{11; 802}	{11; 799}

Схема Блэкли						
X1	X2	X3	X4	X5	X6	
{16, 7, 14, 3402}	{16, 7, 14, 3226}	{16, 7, 14, 3434}	{16, 7, 14, 3290}	{16, 7, 14, 3658}	{16, 7, 14, 3610}	
{12, 10, 24, 2692}	{12, 10, 24, 2560}	{12, 10, 24, 2716}	{12, 10, 24, 2608}	{12, 10, 24, 2884}	{12, 10, 24, 2848}	
{14, 30, 24, 3178}	{14, 30, 24, 3024}	{14, 30, 24, 3206}	{14, 30, 24, 3080}	{14, 30, 24, 3402}	{14, 30, 24, 3360}	
{28, 6, 17, 5861}	{28, 6, 17, 5553}	{28, 6, 17, 5917}	{28, 6, 17, 5665}	{28, 6, 17, 6309}	{28, 6, 17, 6225}	
{20, 4, 28, 4328}	{20, 4, 28, 4108}	{20, 4, 28, 4368}	{20, 4, 28, 4188}	{20, 4, 28, 4648}	{20, 4, 28, 4588}	
Схема Шамира						
X1	X2	X3	X4	X5	X6	
{1; 211}	{1; 205}	{1; 204}	{1; 213}	{1; 208}	{1; 210}	
{8; 435}	{8; 429}	{8; 428}	{8; 437}	{8; 432}	{8; 434}	
{9; 491}	{9; 485}	{9; 484}	{9; 493}	{9; 488}	{9; 490}	
{10; 553}	{10; 547}	{10; 546}	{10; 555}	{10; 550}	{10; 552}	
{14; 861}	{14; 855}	{14; 854}	{14; 863}	{14; 858}	{14; 860}	
Схема Блэкли						
X1	X2	X3	X4	X5	X6	
{19, 3, 9, 3911}	{19, 3, 9, 3797}	{19, 3, 9, 3778}	{19, 3, 9, 3949}	{19, 3, 9, 3854}	{19, 3, 9, 3892}	
{3, 23, 25, 803}	{3, 23, 25, 785}	{3, 23, 25, 782}	{3, 23, 25, 809}	{3, 23, 25, 794}	{3, 23, 25, 800}	
{16, 27, 26, 3459}	{16, 27, 26, 3363}	{16, 27, 26, 3347}	{16, 27, 26, 3491}	{16, 27, 26, 3411}	{16, 27, 26, 3443}	
{11, 1, 4, 2256}	{11, 1, 4, 2190}	{11, 1, 4, 2179}	{11, 1, 4, 2278}	{11, 1, 4, 2223}	{11, 1, 4, 2245}	
{11, 25, 6, 2338}	{11, 25, 6, 2272}	{11, 25, 6, 2261}	{11, 25, 6, 2360}	{11, 25, 6, 2305}	{11, 25, 6, 2327}	
Схема Шамира						
X1	X2	X3	X4	X5	X6	
{1; 217}	{1; 205}	{1; 215}	{1; 213}	{1; 236}	{1; 211}	
{3; 267}	{3; 255}	{3; 265}	{3; 263}	{3; 286}	{3; 261}	
{8; 532}	{8; 520}	{8; 530}	{8; 528}	{8; 551}	{8; 526}	
{10; 694}	{10; 682}	{10; 692}	{10; 690}	{10; 713}	{10; 688}	
{11; 787}	{11; 775}	{11; 785}	{11; 783}	{11; 806}	{11; 781}	
Схема Блэкли						
X1	X2	X3	X4	X5	X6	
{4, 21, 18, 1062}	{4, 21, 18, 1014}	{4, 21, 18, 1054}	{4, 21, 18, 1046}	{4, 21, 18, 1138}	{4, 21, 18, 1038}	
{5, 23, 2, 1130}	{5, 23, 2, 1070}	{5, 23, 2, 1120}	{5, 23, 2, 1110}	{5, 23, 2, 1225}	{5, 23, 2, 1100}	
{26, 30, 1, 5433}	{26, 30, 1, 5121}	{26, 30, 1, 5381}	{26, 30, 1, 5329}	{26, 30, 1, 5927}	{26, 30, 1, 5277}	

	{24, 20, 19, 5147}	{24, 20, 19, 4859}	{24, 20, 19, 5099}	{24, 20, 19, 5051}	{24, 20, 19, 5603}	{24, 20, 19, 5003}
	{30, 14, 3, 6203}	{30, 14, 3, 5843}	{30, 14, 3, 6143}	{30, 14, 3, 6083}	{30, 14, 3, 6773}	{30, 14, 3, 6023}
	Схема Шамира					
	X1	X2	X3	X4	X5	X6
	{1; 228}	{1; 216}	{1; 232}	{1; 226}	{1; 224}	{1; 225}
	{2; 272}	{2; 260}	{2; 276}	{2; 270}	{2; 268}	{2; 269}
	{8; 956}	{8; 944}	{8; 960}	{8; 954}	{8; 952}	{8; 953}
	{10; 1344}	{10; 1332}	{10; 1348}	{10; 1342}	{10; 1340}	{10; 1341}
	{12; 1812}	{12; 1800}	{12; 1816}	{12; 1810}	{12; 1808}	{12; 1809}
20)	X1	X2	X3	X4	X5	X6
	{26, 30, 16, 5828}	{26, 30, 16, 5516}	{26, 30, 16, 5932}	{26, 30, 16, 5776}	{26, 30, 16, 5724}	{26, 30, 16, 5750}
	{22, 24, 1, 4742}	{22, 24, 1, 4478}	{22, 24, 1, 4830}	{22, 24, 1, 4698}	{22, 24, 1, 4654}	{22, 24, 1, 4676}
	{23, 1, 10, 4842}	{23, 1, 10, 4566}	{23, 1, 10, 4934}	{23, 1, 10, 4796}	{23, 1, 10, 4750}	{23, 1, 10, 4773}
	{6, 6, 22, 1592}	{6, 6, 22, 1520}	{6, 6, 22, 1616}	{6, 6, 22, 1580}	{6, 6, 22, 1568}	{6, 6, 22, 1574}
	{29, 5, 17, 6204}	{29, 5, 17, 5856}	{29, 5, 17, 6320}	{29, 5, 17, 6146}	{29, 5, 17, 6088}	{29, 5, 17, 6117}

### Содержание отчета

- 1) Титульный лист (Пример в приложении В).
- 2) Цель работы.
- 3) Задание, примеры расчетов, вычисления.
- 4) Разделенное и восстановленное сообщение.
- 5) Выводы.

### Контрольные вопросы

- 1) Поясните концепцию разбиения данных. Приведите пример.
- 2) Поясните концепцию порогового разделения данных. Приведите пример.
- 3) Расскажите принцип порогового разделения данных с применением схемы Шамира.
- 4) Расскажите принцип порогового разделения данных с применением схемы Блэкли.

## Литература

5) Титов, А. А. Инженерно-техническая защита информации: учебное пособие / А. А. Титов. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/13931.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

6) Литвинов, Р. В. Технические средства защиты информации. Часть 1: курс лекций / Р. В. Литвинов, К. А. Волегов, А. П. Бацула. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2006. — 170 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/14027.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

7) Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 95 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17925.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

8) Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 104 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17926.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

## Тема 6. Методы защиты информации с применением методов основанных на разделении данных

### Лабораторная работа №6 «Изучение математических моделей схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации»

**Цель работы:** изучить принцип работы алгоритмов порогового разделения данных основанных на системе остаточных классов и численные методы их реализации.

#### Программа работы

1) Изучить теоретический материал, математические и алгоритмические особенности схем порогового разделения данных основанных на системе остаточных классов.

2) В соответствии с заданием построить математическую модель алгоритма порогового разделения данных, основанного на системе остаточных классов.

#### Элементы теории

Система остаточных классов (СОК) это непозиционная система счисления, основанная на модулярной арифметике. Представление чисел в СОК основано на понятии вычета и Китайской теореме об остатках.

СОК определяется рядом попарно взаимно простых модулей  $(p_1, p_2, \dots, p_n)$ , таких, что  $\text{gnd}(p_i, p_j) = 1$  ( $\forall: i, j = 0, 1, 2, \dots, n; i \neq j$ ) называемых базисом при  $P = p_1 \cdot p_2 \cdot \dots \cdot p_n$  таким образом любому целому  $S$  из множества  $[0; P - 1]$  ставится соответствие набор остатков  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  где:

$$\begin{cases} \alpha_1 = S \bmod p_1 \\ \alpha_2 = S \bmod p_2 \\ \dots \\ \alpha_n = S \bmod p_n \end{cases}$$

При этом Китайская теорема об остатках гарантирует однозначность представления целых положительных чисел из диапазона  $[0; P - 1]$ .

Принципы Китайской теоремы об остатках были также применены для разделения секрета и предложены в работах: M. Mignotte. How to Share a Secret // Lecture Notes in Computer Science. — 1983. — Vol. 149. — P. 371—375. — doi:10.1007/3-540-39466-4\_27. и С. А. Asmuth and J. Bloom. A modular approach to key safeguarding // IEEE Transactions on Information Theory. — 1986. — Vol. 2. — P. 208-210

### **Концепция схемы разделения секрета Миньотта**

Схема разделения секрета Миньотта позволяет пользователю, имеющему некоторое разрешенное количество частей секрета, восстановить сам секрет, причем единственным образом.

Принцип работы схемы, следующий: пусть необходимо разделить секрет  $S$  среди  $n$  пользователей таким образом чтобы при условии наличия  $k$  частей, было возможно восстановить исходную информацию, а имея в наличии  $k - 1$  не имели такой возможности.

Для этого необходима последовательность натуральных чисел (называемую  $(k, n)$ -последовательностью Миньотта) такая, что:  $p_1 < p_2 < \dots < p_n$  и  $\prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^k p_i$ . Причем должны соблюдаться следующие условия:

- любые два числа последовательности должны быть взаимно простыми т.е.  $\text{gcd}(p_i, p_j) = 1$  ( $\forall: i, j = 0, 1, 2, \dots, n; i \neq j$ );

- секрет должен находиться в диапазоне  $\alpha < S < \beta$  где:  $\alpha = \prod_{i=1}^k p_i$ , а  $\beta = \prod_{i=0}^{k-2} p_{n-i}$  то есть  $p_1 \cdot p_2 \cdot \dots \cdot p_k < S < p_{n-k+2} \cdot p_{n-k+3} \cdot \dots \cdot p_n$ .

Части вычисляются по формуле  $\alpha_i = S \bmod p_i$  для всех  $i \in [1; n]$  и распределяются среди пользователей.

Восстановление данных может производиться разными способами, такими как: метод основанный на Китайской теореме об остатках; метод основанный на обобщенной полиадической системе счисления; метод основанный на совместном использовании китайской теоремы об остатках и обобщенной полиадической системе счисления и других методах.

Наиболее простым для понимания является метод, основанный на Китайской теореме об остатках. В ней любое число представляется в виде:

$$S = (\alpha_1\beta_1 + \alpha_2\beta_2 + \dots + \alpha_k\beta_k) \bmod P$$

где:  $\alpha_i$  – часть секрета;  $\beta_i$  – базис;  $P = p_1 \cdot p_2 \cdot \dots \cdot p_k$  – диапазон СОК.

Базис вычисляется по формуле:

$$\beta_i = m_i P_i$$

где:  $P_i = \frac{P}{p_i}$ ;  $m_i$  – вес базиса, вычисляется из приближения:

$$m_i P_i \bmod p_i = 1$$

### Пример реализации схемы Миньотта

Пусть необходимо разделить секретную информацию  $S = 250$  применив  $(k, n)$  схему Миньотта для  $k = 3$  и  $n = 5$ .

Для этого необходимо выбрать ряд попарно простых модулей, удовлетворяющих условию  $\beta = \prod_{i=0}^{k-2} p_{n-i} < 250 < \alpha = \prod_{i=1}^k p_i$ .

Из ряда простых чисел примем следующий набор оснований СОК:  $p_1 = 5$ ;  $p_2 = 7$ ;  $p_3 = 11$ ;  $p_4 = 13$ ;  $p_5 = 17$ . Проводится проверка на соответствие выбранных оснований с неравенством:

$$5 \cdot 7 \cdot 11 < 250 < 13 \cdot 17$$

Следующим этапом  $S = 250$  разделяется на  $n$  частей:

$$\alpha_1 = 250 \bmod 5 = 0;$$

$$\alpha_2 = 250 \bmod 7 = 5;$$

$$\alpha_3 = 250 \bmod 11 = 8;$$

$$\alpha_4 = 250 \bmod 13 = 3;$$

$$\alpha_5 = 250 \bmod 17 = 12.$$

Далее части распространяются среди пользователей.

Восстанавливается секрета по  $k = 3$  частям для  $\alpha_1 = 0$ ;  $\alpha_3 = 8$ ;  $\alpha_5 = 12$ .

Для выбранных частей диапазон СОК равен  $P = p_1 \cdot p_3 \cdot p_5 = 5 \cdot 11 \cdot 17 = 935$ , тогда:

$$P_1 = \frac{P}{p_1} = \frac{935}{5} = 187;$$

$$P_3 = \frac{P}{p_3} = \frac{935}{11} = 85;$$

$$P_5 = \frac{P}{p_5} = \frac{935}{17} = 55.$$

Зная  $P_1, P_3, P_5$  рассчитываются веса базисов:

$$m_1 187 \bmod 5 = 1 \text{ тогда } m_1 = 3;$$

$$m_3 85 \bmod 11 = 1 \text{ тогда } m_3 = 7;$$

$$m_5 55 \bmod 17 = 1 \text{ тогда } m_5 = 13.$$

Тогда базисы:

$$\beta_1 = m_1 P_1 = 187 \cdot 3 = 561;$$

$$\beta_3 = m_3 P_3 = 85 \cdot 7 = 595;$$

$$\beta_5 = m_5 P_5 = 55 \cdot 13 = 715;$$

Зная все коэффициенты, можно восстановить секрет. Тогда:

$$S = (0 \cdot 561 + 8 \cdot 595 + 12 \cdot 715) \bmod 935 = 250.$$

### **Концепция схемы разделения секрета Асмута-Блума**

Схема Асмута-Блума, как и схема Миньотта это пороговая схема разделения секрета, построенная с использованием ряда простых чисел которая позволяет разделить секрет среди  $n$  сторон так что его восстановят любые  $k$  участников.

Для разделения секрета схемой Асмута-Блума необходимо выбрать простое число  $q$  больше  $S$ .

Следующим этапом проводится выбор  $n$  взаимно простых друг с другом чисел  $p_1, p_2, \dots, p_n$  удовлетворяющих следующим условиям:

- $\forall i: q < p_i$ ;
- $\forall i: p_i < p_{i+1}$ ;
- $p_1 \cdot p_2 \cdot \dots \cdot p_k < q \cdot p_{n-k+2} \cdot p_{n-k+3} \cdot \dots \cdot p_n$ .

Далее необходимо выбрать случайное число  $r$  и вычислить  $S' = S + r \cdot q$ .

Части секрета вычисляются по формуле  $\alpha_i = S' \bmod p_i$ . Участникам раздается следующая информация  $\{q, p_i, \alpha_i\}$ .



Восстановление данных может производиться разными способами такими как: метод основанный на Китайской теореме об остатках; метод основанный на обобщенной полиадической системе счисления; метод основанный на совместном использовании китайской теоремы об остатках и обобщенной полиадической системе счисления и других методах.

Для преобразования из системы остаточных классов в позиционную систему счисления кроме Китайской теоремы об остатках, также широко применяется метод на основе обобщенной полиадической системы счисления.

В обобщенной полиадической системе счисления число  $A$  представляется в виде:

$$A = a_1 + a_2 p_1 + a_3 p_1 p_2 + \dots + a_n p_1 p_2 \dots p_{n-1}$$

где  $a_i$  – коэффициенты обобщенной полиадической системы счисления. Также эту формулу можно записать в виде:

$$A = a_1 + p_1(a_2 + p_2(a_3 + \dots + p_{n-2}(a_{n-1} + p_{n-1}a_n) \dots))$$

Из этой формулы видно, что коэффициенты обобщенной полиадической системы счисления могут быть получены из отношений:

$$a_1 = A - \left\lfloor \frac{A}{p_1} \right\rfloor p_1 = A - A_1 p_1 \quad \text{где } A_1 = \left\lfloor \frac{A}{p_1} \right\rfloor$$

$$a_2 = A_1 - \left\lfloor \frac{A_1}{p_2} \right\rfloor p_2 = A_1 - A_2 p_2 \quad \text{где } A_2 = \left\lfloor \frac{A_1}{p_2} \right\rfloor$$

...

$$a_n = A_{n-1} - \left\lfloor \frac{A_{n-1}}{p_n} \right\rfloor p_n = A_{n-1} - A_n p_n \quad \text{где } A_n = \left\lfloor \frac{A_{n-1}}{p_n} \right\rfloor$$

Из этих отношений следует что  $a_1 = |A|_{p_1}$  то есть  $a_1 = \alpha_1$ . Для вычисления  $a_2$ , разность  $A - a_1$  вычисляется в остаточном коде. Очевидно, что  $A - a_1$  делится на  $p_1$ , а  $p_1$  взаимно простое число с другими модулями из ряда  $p_1, p_2, \dots, p_n$ . Из этого следует что для нахождения коэффициента  $a_2$  используют процедуру деления без остатка  $a_2 = \left| \frac{A - a_1}{p_1} \right|_{p_2}$ . Зная эту процедуру, могут быть получены все коэффициенты обобщенной полиадической системы счисления с применением простых арифметических операций «вычитание» и «деление»:

$$a_1 = |A|_{p_1}, a_2 = \left| \frac{A-a_1}{p_1} \right|_{p_2}, a_3 = \left| \frac{A-a_2}{p_2} \right|_{p_3} \dots \text{ для } i > 0 \ a_i = \left| \frac{A}{p_1 p_2 \dots p_{i-1}} \right|_{p_i}$$

Перевод, осуществляемый с помощью этого алгоритма, содержит  $2(n-1)$  операций «вычитание» и «деление» без остатка.

Модифицировать этот алгоритм можно заменив операцию «деление» операцией «умножения». Для этого необходимо вычислить константы  $\tau_{k,j}$ , удовлетворяющие условию  $\tau_{k,i} p_k \equiv 1 \pmod{p_i}, 1 \leq k < i \leq n$ .

Эти константы  $\tau_{k,i}$  зависят от выбранной системы счисления и вычисляются в самом начале.

Если имеются константы  $\tau_{k,i}$  то коэффициенты  $a_i$  вычисляются следующим образом:

$$a_1 = \alpha_1 \pmod{p_2};$$

$$a_2 = (\alpha_2 - a_1) \tau_{1,2} \pmod{p_2};$$

$$a_3 = ((\alpha_3 - a_1) \tau_{1,3} - a_2) \tau_{2,3} \pmod{p_3};$$

...

$$a_n = (((\dots (\alpha_n - a_{n-1}) \tau_{1,n} - a_2) \tau_{2,n} \dots) \tau_{n-1,n}) \pmod{p_n};$$

Константы  $\tau_{k,i}$  также можно представить в виде  $\tau_{k,i} = \left| \frac{1}{p_k} \right|_{p_i}$ .

### Пример реализации схемы Асмута-Блума

Пусть необходимо разделить секретную информацию  $S = 250$  применив  $(k, n)$  схему Асмута-Блума для  $k = 3$  и  $n = 5$ .

Производится выбор простого числа в соответствии с условием:  $q > S$  тогда примем  $q = 257$ .

Далее необходимо произвести выбор ряда взаимно простых чисел таких что:  $p_1 \cdot p_2 \cdot \dots \cdot p_k < q \cdot p_{n-k+2} \cdot p_{n-k+3} \cdot \dots \cdot p_n, \forall i: p_i < p_{i+1}$  и  $\forall i: q < p_i$  тогда  $p_1 = 263, p_2 = 269, p_3 = 271, p_4 = 277, p_5 = 281$ .

Приняв константу  $r = 15$  рассчитывается  $S' = 250 + 15 \cdot 257 = 4105$ . Тогда части секрета равны:

$$- \quad \alpha_1 = 4105 \pmod{263} = 160;$$

- $\alpha_2 = 4105 \bmod 269 = 70$ ;
- $\alpha_3 = 4105 \bmod 271 = 40$ ;
- $\alpha_4 = 4105 \bmod 277 = 227$ ;
- $\alpha_5 = 4105 \bmod 281 = 171$ .

Далее восстанавливается секрет по  $k = 3$  частям для  $\alpha_1 = 70$ ;  $\alpha_2 = 40$ ;  $\alpha_3 = 171$ .

Для выбранных частей основания системы остаточных классов, следующие:  $p_1 = 269$ ,  $p_2 = 271$ ,  $p_3 = 281$ .

Тогда константы  $\tau_{k,i}$  равны:

$$\tau_{1,2} = \left| \frac{1}{269} \right|_{271} = 135; \quad \tau_{1,3} = \left| \frac{1}{269} \right|_{281} = 117;$$

$$\tau_{2,3} = \left| \frac{1}{271} \right|_{281} = 28;$$

Зная константы  $\tau_{k,i}$  вычисляются коэффициенты обобщенной полиадической системы счисления:

$$a_1 = 70 \bmod 269 = 70;$$

$$a_2 = (40 - 70)135 \bmod 271 = 15;$$

$$a_3 = ((171 - 70)117 - 15)28 \bmod 281 = 0;$$

Далее восстанавливается  $S'$ :

$$S' = 70 + 15 \cdot 269 + 0 \cdot 269 \cdot 271 = 4105$$

Тогда секрет  $S'$  равен  $S' = 4105 - 15 \cdot 257 = 250$ .

### **Указания по технике безопасности**

В начале каждого семестра, со студентами должен проводиться инструктаж по технике безопасности в лаборатории. Во время нахождения студента в лаборатории и выполнения лабораторных работ студент не должен нарушать инструкции по охране труда с персональным компьютером ИОТ-37-ИВЛ-19, и инструкцию о мерах пожарной безопасности ИБП-01-2016.

### **Методические указания к выполнению работы**

Каждому студенту для слов, представленных в таблице (6.1) в соответствии с вариантом необходимо реализовать  $(k, n)$  пороговые схемы

разделения данных Миньотта и Асмута-Блума при  $k \neq n$ . В отчете необходимо показать процесс разделения и восстановления секрета используя  $k$  частей и  $n$  частей.

При выполнении работы разрешается использовать любые технические и программные средства.

Таблица 6.1 – Задания для выполнения работы

№ варианта	Задание
1	АНКЛАВ
2	АРМАДА
3	БЕСЕДА
4	БЕСИТЬ
5	ВЗВЕСЬ
6	ВЗГЛЯД
7	ГЕКТАР
8	ГЕЙЗЕР
9	ДЕВИЦА
10	ДЕКАДА
11	ЗАДАТЬ
12	ЗАЖАТЬ
13	ЗАМЯТЬ
14	ИНТЕРН
15	КАПКАН
16	КАПРОН
17	ЛЕКАРЬ
18	ЛЕКТОР
19	НАДЗОР
20	НАДРЕЗ

### Содержание отчета

- 1) Титульный лист (Пример в приложении В).
- 2) Цель работы.
- 3) Задание, примеры расчетов, вычисления.
- 4) Разделенное и восстановленное сообщение.
- 5) Расчеты.
- 6) Выводы.

## **Контрольные вопросы**

- 1) Поясните преимущества использование системы остаточных классов для разделения секрета.
- 2) Каким образом информация из системы остаточных классов переводится в десятичную систему счисления с применением обобщенной полиадической системы счисления.
- 3) Расскажите принцип порогового разделения данных с применением схемы Миньотта.
- 4) Расскажите принцип порогового разделения данных с применением схемы Асмута-Блума.

## **Литература**

- 1) Титов, А. А. Инженерно-техническая защита информации: учебное пособие / А. А. Титов. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/13931.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей
- 2) Литвинов, Р. В. Технические средства защиты информации. Часть 1: курс лекций / Р. В. Литвинов, К. А. Волегов, А. П. Бацула. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2006. — 170 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/14027.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей
- 3) Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 95 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17925.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

4) Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 104 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/17926.html> (дата обращения: 04.12.2020). — Режим доступа: для авторизир. Пользователей

## Приложение А – Таблица частот биграмм русского языка

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	
А	2	12	35	8	14	7	6	15	7	7	19	27	19	45	3	11	26	31	27	3	1	10	6	7	10	1			2	6	9	
Б	5					9	1		6			6		2	21		8	1		6					1	11					2	
В	35	1	5	3	3	32		2	17		7	10	3	9	58	6	6	19	6	7		1	1	2	4	1	18	1	2		3	
Г	7				3	3			5		1	5		1	50		7			2												
Д	25		3	1	1	29	1	1	13		1	5	1	13	22	3	6	8	1	10			1	1	1		5	1			1	
Е	2	9	18	11	27	7	5	10	6	15	13	35	24	63	7	16	39	37	33	3	1	8	3	7	3	3			1	1	2	
Ж	5	1			6	12			5					6				1														
З	35	1	7	1	5	3			4		2	1	2	9	9	1	3	1		2							4				4	
И	4	6	22	5	10	21	2	23	19	11	19	21	20	32	8	13	11	29	29	3	1	17	1	11	1	1			1	3	17	
Й	1	1	4	1	3		1	2	4		5	1	2	7	9	7	3	10	2				1	3	2							
К	24	1	4	1		4	1	1	26		1	4	1	2	66	2	10	3	7	10			1									
Л	25	1	1	1	1	33	2	1	36		1	2	1	8	30	2		3	1	6		4		1			2	30		4	9	
М	18	2	4	1	1	21	1	2	33		3	1	3	7	19	5	2	5	3	9	1			2			5	1	1		3	
Н	54	1	2	3	3	34			58		3		1	24	67	2	1	9	9	7	1		5	2			36	3			5	
О	1	28	84	32	47	15	7	18	12	29	19	41	38	30	9	18	43	50	39	3	2	5	2	12	4	3			2	3	2	
П	7					15			4			9		1	46		41	1		6							2				2	
Р	55	1	4	4	3	37	3	1	24		3	1	3	7	56	2	1	5	9	16		1	1	1	2		8	3			5	
С	8	1	7	1	2	25			6		40	13	3	9	27	11	4	11	82	6		1	1	2	2		1	8			17	
Т	35	1	27	1	3	31		1	28		5	1	1	11	56	4	26	18	2	10				1			11	21			4	
У	1	4	4	4	11	2	6	3	2		8	5	5	5	1	5	7	14	7			1		8	3	2				9	1	
Ф	2					2			2						1		1	1														
Х	4	1	4	1	3	1		2	3		4	3	3	4	18	5	3	4	2	2	1			1								
Ц	3					7			10		2				1					1							1					
Ч	12					23			13		2			6					7	1					1			1				
Ш	5					11			14		1	2		2	2					1								1				
Щ	3					8			6					1						1												
Ы		1	9	1	3	12		2	4	7	3	6	6	3	2	10	3	9	4	1		16		1	2							
Ь		2	4	1	1	2		2	2		6		3	13	2	4	1	11	3					1	4				1	3	1	
Э											1			1				1	9													
Ю		2	1	2	1			3	1		1		1	1	1	3	1	1	7				1	1		4						
Я	1	3	9	1	3	3	1	5	3	2	3	3	4	6	3	6	3	6	10			2	1	4	1	1			1	1	1	

## Приложение Б – Таблица ASCII кодов

ASCII	Символ	ASCII	Символ	ASCII	Символ	ASCII	Символ	ASCII	Символ	ASCII	Символ	ASCII	Символ	ASCII	Символ
0	NUL	32	Space	64	@	96	`	128	Ђ	160	Ў	192	А	224	а
1	SOH	33	!	65	A	97	a	129	Ѓ	161	ў	193	Б	225	б
2	STX	34	"	66	B	98	b	130	,	162	Ј	194	В	226	в
3	ETX	35	#	67	C	99	c	131	ѓ	163	ѡ	195	Г	227	г
4	EOT	36	\$	68	D	100	d	132	„	164	Ѕ	196	Д	228	д
5	ENQ	37	%	69	E	101	e	133	…	165	Ї	197	Е	229	е
6	ACK	38	&	70	F	102	f	134	†	166	§	198	Ж	230	ж
7	BEL	39	'	71	G	103	g	135	‡	167	Ё	199	З	231	з
8	BS	40	(	72	H	104	h	136	€	168	©	200	И	232	и
9	TAB	41	)	73	I	105	i	137	‰	169	€	201	Й	233	й
10	LF	42	*	74	J	106	j	138	Љ	170	«	202	К	234	к
11	VT	43	+	75	K	107	k	139	‹	171	¬	203	Л	235	л
12	FF	44	,	76	L	108	l	140	Њ	172		204	М	236	м
13	CR	45	-	77	M	109	m	141	Ћ	173	®	205	Н	237	н
14	SO	46	.	78	N	110	n	142	ћ	174	İ	206	О	238	о
15	SI	47	/	79	O	111	o	143	Ѡ	175	°	207	П	239	п
16	DLE	48	0	80	P	112	p	144	ђ	176	±	208	Р	240	р
17	DC1	49	1	81	Q	113	q	145	‘	177	І	209	С	241	с
18	DC2	50	2	82	R	114	r	146	’	178	і	210	Т	242	т
19	DC3	51	3	83	S	115	s	147	“	179	г	211	У	243	у
20	DC4	52	4	84	T	116	t	148	”	180	μ	212	Ф	244	ф
21	NAK	53	5	85	U	117	u	149	•	181	¶	213	Х	245	х
22	SYN	54	6	86	V	118	v	150	–	182	·	214	Ц	246	ц
23	ETB	55	7	87	W	119	w	151	—	183	ë	215	Ч	247	ч
24	CAN	56	8	88	X	120	x	152	?	184	№	216	Ш	248	ш
25	EM	57	9	89	Y	121	y	153	™	185	е	217	Щ	249	щ
26	SUB	58	:	90	Z	122	z	154	љ	186	»	218	Ъ	250	ъ
27	ESC	59	;	91	[	123	~	155	›	187	ј	219	Ы	251	ы
28	FS	60	<	92	\	124	DEL	156	њ	188	ѕ	220	Ь	252	ь
29	GS	61	=	93	]	125		157	ќ	189	s	221	Э	253	э
30	RS	62	>	94	^	126		158	ћ	190	ï	222	Ю	254	ю
31	US	63	?	95	_	127		159	ѡ	191		223	Я	255	я



## **Пример в приложении В – Форма титульного листа**

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**  
Федеральное государственное автономное образовательное учреждение  
высшего образования  
**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**  
Невинномысский технологический институт (филиал)  
Базовая кафедра Регионального индустриального парка

Лабораторная Работа №1  
«Изучение математических моделей шифра простой замены»  
По дисциплине «Персональная кибербезопасность»

Выполнил (-а) Фамилия Имя Отчество  
студент(ка) 1 курса, группы Н-АТП-б-о-21-1  
направление подготовки/специальность  
15.03.04 Автоматизация технологических  
процессов и производств  
профиль/специализация Информационно-  
управляющие системы

---

(подпись)

Проверил Фамилия Имя Отчество, доцент  
базовой кафедры Регионального  
индустриального парка

---

(подпись)

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение  
высшего образования  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

# ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ

Методические указания к самостоятельным работам

Направление подготовки 15.03.04 Автоматизация технологических процессов  
и производств

Направленность (профиль) «Информационно-управляющие системы»

Квалификация выпускника – бакалавр

Невинномысск 2022

Методические указания предназначены для студентов направления подготовки 15.03.04 Автоматизация технологических процессов и производств и других технических специальностей. Они содержат рекомендации по организации самостоятельных работ студента для дисциплины «Персональная кибербезопасность».

Методические указания разработаны в соответствии с требованиями ФГОС ВО в части содержания и уровня подготовки выпускников направления 15.03.04 Автоматизация технологических процессов и производств

## Содержание

1 Подготовка к лекциям.....	4
2 Подготовка к лабораторным работам .....	6
3 Самостоятельное изучение темы. Конспект.....	8

## 1 Подготовка к лекциям

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин.

Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность студента. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим студентом. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях.

Конспект лекций лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места, опре-

деления, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось присить их у однокурсников и тем самым не отвлекать их во время лекции. Целесообразно разработать собственную «маркографию» (значки, символы), сокращения слов. Не лишним будет и изучение основ стенографии. Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть знаниями.

## 2 Подготовка к лабораторным работам

Подготовку к каждому практическому занятию студент должен начать с ознакомления с методическими указаниями, которые включают содержание работы. Тщательное продумывание и изучение вопросов основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованную к данной теме. На основе индивидуальных предпочтений студенту необходимо самостоятельно выбрать тему доклада по проблеме и по возможности подготовить по нему презентацию.

Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (устно или письменно). Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы семинара, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

В зависимости от содержания и количества отведенного времени на изучение каждой темы практическое занятие может состоять из четырех-пяти частей:

1. Обсуждение теоретических вопросов, определенных программой дисциплины.
2. Доклад и/ или выступление с презентациями по выбранной проблеме.
3. Обсуждение выступлений по теме – дискуссия.
4. Выполнение практического задания с последующим разбором полученных результатов или обсуждение практического задания.
5. Подведение итогов занятия.

Первая часть – обсуждение теоретических вопросов – проводится в виде фронтальной беседы со всей группой и включает выборочную проверку преподавателем теоретических знаний студентов. Примерная продолжительность — до 15 минут. Вторая часть — выступление студентов с докладами, которые должны сопровождаться презентациями с целью усиления наглядности восприятия, по одному из вопросов практического занятия. Обязательный элемент доклада – представление и анализ статистических данных, обоснование социальных последствий любого экономического факта, явления или процесса. Примерная продолжительность — 20-25 минут. После докладов следует их обсуждение – дискуссия. В ходе этого этапа практического занятия могут быть заданы уточняющие вопросы к докладчикам. Примерная продолжительность – до 15-20 минут. Если программой предусмотрено выполнение практического задания в рамках конкретной темы, то преподавателями определяется его содержание и дается время на его выполнение, а затем идет обсуждение результатов. Подведением итогов заканчивается практическое занятие.

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме семинарского или практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.



### 3 Самостоятельное изучение темы. Конспект

Конспект – наиболее совершенная и наиболее сложная форма записи. Слово «конспект» происходит от латинского «conspectus», что означает «обзор, изложение». В правильно составленном конспекте обычно выделено самое основное в изучаемом тексте, сосредоточено внимание на наиболее существенном, в кратких и четких формулировках обобщены важные теоретические положения.

Конспект представляет собой относительно подробное, последовательное изложение содержания прочитанного. На первых порах целесообразно в записях ближе держаться тексту, прибегая зачастую к прямому цитированию автора. В дальнейшем, по мере выработки навыков конспектирования, записи будут носить более свободный и сжатый характер.

Конспект книги обычно ведется в тетради. В самом начале конспекта указывается фамилия автора, полное название произведения, издательство, год и место издания. При цитировании обязательная ссылка на страницу книги. Если цитата взята из собрания сочинений, то необходимо указать соответствующий том. Следует помнить, что четкая ссылка на источник – неперемutable правило конспектирования. Если конспектируется статья, то указывается, где и когда она была напечатана.

Конспект подразделяется на части в соответствии с заранее продуманным планом. Пункты плана записываются в тексте или на полях конспекта. Писать его рекомендуется четко и разборчиво, так как небрежная запись с течением времени становится малопонятной для ее автора. Существует правило: конспект, составленный для себя, должен быть по возможности написан так, чтобы его легко прочитал и кто-либо другой.

Формы конспекта могут быть разными и зависят от его целевого назначения (изучение материала в целом или под определенным углом зрения, подготовка к докладу, выступлению на занятии и т.д.), а также от характера произведения (монография, статья, документ и т.п.). Если речь идет просто об изложении содержания работы, текст конспекта может быть сплошным, с

выделением особо важных положений подчеркиванием или различными значками.

В случае, когда не ограничиваются переложением содержания, а фиксируют в конспекте и свои собственные суждения по данному вопросу или дополняют конспект соответствующими материалами их других источников, следует отводить место для такого рода записей. Рекомендуется разделить страницы тетради пополам по вертикали и в левой части вести конспект произведения, а в правой свои дополнительные записи, совмещая их по содержанию.

Конспектирование в большей мере, чем другие виды записей, помогает вырабатывать навыки правильного изложения в письменной форме важные теоретических и практических вопросов, умение четко их формулировать и ясно излагать своими словами.

Таким образом, составление конспекта требует вдумчивой работы, затраты времени и труда. Зато во время конспектирования приобретаются знания, создается фонд записей.

Конспект может быть текстуальным или тематическим. В текстуальном конспекте сохраняется логика и структура изучаемого произведения, а запись ведется в соответствии с расположением материала в книге. За основу тематического конспекта берется не план произведения, а содержание какой-либо темы или проблемы.

Текстуальный конспект желательно начинать после того, как вся книга прочитана и продумана, но это, к сожалению, не всегда возможно. В первую очередь необходимо составить план произведения письменно или мысленно, поскольку в соответствии с этим планом строится дальнейшая работа. Конспект включает в себя тезисы, которые составляют его основу. Но, в отличие от тезисов, конспект содержит краткую запись не только выводов, но и доказательств, вплоть до фактического материала. Иначе говоря, конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, мыслями и соображениями составителя записи.

Как правило, конспект включает в себя и выписки, но в него могут войти отдельные места, цитируемые дословно, а также факты, примеры, цифры, таблицы и схемы, взятые из книги. Следует помнить, что работа над конспектом только тогда будет творческой, когда она не ограничена текстом изучаемого произведения. Нужно дополнять конспект данными из другими источниками.

В конспекте необходимо выделять отдельные места текста в зависимости от их значимости. Можно пользоваться различными способами: подчеркиваниями, вопросительными и восклицательными знаками, репликами, краткими оценками, писать на полях своих конспектов слова: «важно», «очень важно», «верно», «характерно».

В конспект могут помещаться диаграммы, схемы, таблицы, которые придадут ему наглядность.

Составлению тематического конспекта предшествует тщательное изучение всей литературы, подобранной для раскрытия данной темы. Бывает, что какая-либо тема рассматривается в нескольких главах или в разных местах книги. А в конспекте весь материал, относящийся к теме, будет сосредоточен в одном месте. В плане конспекта рекомендуется делать пометки, к каким источникам (вплоть до страницы) придется обратиться для раскрытия вопросов. Тематический конспект составляется обычно для того, чтобы глубже изучить определенный вопрос, подготовиться к докладу, лекции или выступлению на семинарском занятии. Такой конспект по содержанию приближается к реферату, докладу по избранной теме, особенно если включает и собственный вклад в изучение проблемы.