Министерство науки и высшего образования Российской Федерации
Университетский колледж
федерального государственного бюджетного образовательного учреждения
высшего образования
«Оренбургский государственный университет»

Н.А. Кривошеева

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы

Оренбург
2019

УДК 002.56:681(075.32)
ББК 32.97я723
К82

Рецензент – доцент кафедры программного обеспечения вычислительной техники и автоматизированных систем И.А. Щудро

Кривошеева, Н.А.

К82 Методы и средства защиты информации: методические указания / Н.А. Кривошеева; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2019. – 32 с.

Методические указания предназначены для выполнения лабораторных работ по дисциплине «Методы и средства защиты информации» в Университетском колледже ОГУ для обучающихся четвертого курса специальности 09.02.01 Компьютерные системы и комплексы.

Методические указания составлены с учетом Федерального государственного образовательного стандарта среднего профессионального образования.

УДК 002.56:681(075.32)
ББК 32.97я723

Содержание

Введение 4
1 Лабораторная работа № 1. Шифрование с использованием системы Цезаря 5
1.1 Теоретические сведения 5
1.2 Практическая часть работы 6
1.3 Вопросы для защиты лабораторной работы № 1 6
2 Лабораторная работа № 2. Шифрование с использованием системы Вижинера 6
2.1 Теоретические сведения 7
2.2 Практическая часть работы 8
2.3 Вопросы для защиты лабораторной работы № 2 11
3 Лабораторная работа № 3. Криптоанализ шифров простой замены 12
3.1 Теоретические сведения 12
3.2 Практическая часть работы 14
3.3 Вопросы для защиты лабораторной работы № 3 17
4 Лабораторная работа № 4. Изучение классических шифров замены 18
4.1 Практическая часть работы 18
4.2 Вопросы для защиты лабораторной работы № 4 26
5 Контрольные вопросы и задания по разделу 26
6 Задачи по разделу 27
7 Тестовые задания 28
Список использованных источников 31
Приложение А 32

Введение

При современном темпе развития компьютерных и цифровых технологий мы не в состоянии воспринимать свою жизнь вне информационного потока окружающего нас. В условиях всеобщей информатизации, вопросы информационной безопасности и защиты информации становятся наиболее актуальными. Наука отайной передачи информации, недоступной илинепонятнойдля посторонних лицстала развиваться в тот момент, когда человечество осознало необходимость обеспечения защиты информации.

Криптография – одна из старейших наук, за время своего существования она претерпела огромное количество изменений, постоянно совершенствуясь и дополняясь. Криптографическая защита информации является одной из основных подсистем любой системы защиты информации. Использование криптографии в современных цифровых технологиях становится неотъемлемой частью многих сфер жизни нашего общества. Этот процесс становится все более и более масштабным. Все чаще в нашей повседневной жизни встречаются такие понятия, как логин и пароль, аутентификация и идентификация, электронная цифровая подпись, шифрование открытым и закрытым ключом, и многие другие. В методических указаниях рассмотрены общие вопросы обеспечения криптографической защиты информации, основные алгоритмы шифрования изложены простыми, понятными способами, в доступной форме изложены основные сведения об основных направлениях криптографии. Последовательность изложения материала в методических указаниях, дополненного иллюстративным материалом, облегчает восприятие дисциплины для обучающихся специальности 09.02.01 Компьютерные системы и комплексы.

1 Лабораторная работа № 1. Шифрование с использованием системы Цезаря

Цель работы: формирование умений шифрования с использованием системы Цезаря.

1.1 Теоретические сведения

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифрах простой замены (одноалфавитной подстановки) каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста.

Система шифрования Цезаря Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). Ключом шифрования является целое число 1 … N, где N – количество букв алфавита шифруемого слова, уменьшенное на 1. Ключ будет обозначаться символом К. При шифровании исходного текста каждая буква заменяется на другую букву того же алфавита. Заменяющая буква определяется путем смещения от исходной буквы алфавита на К букв. При достижении конца алфавита выполняется циклический переход к его началу. Рассмотрим пример шифрования сообщения «ПРИЛЕТАЮ ЗАВТРА» с использованием системы Цезаря. Ключ шифрования К=3. Сначала сформируем таблицу подстановок, содержащую соответствующие пары букв исходного текста и шифртекста (рисунок 1).

Верхняя строка – основной алфавит

а	**б**	**в**	**г**	**д**	**е**	**ё**	**ж**	**з**	**и**	**й**	**к**	**л**	**м**	**н**	**о**	**п**	**р**	**с**	**т**	**у**	**ф**	**х**	**ц**	**ч**	**ш**	**щ**	**ъ**	**ы**	**ь**	**э**	**ю**	**я**
г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в

Нижняя строка – алфавит, сдвинутый вправо по ключу 3

Рисунок 1 – Таблица подстановок для системы Цезаря

При шифровании каждая буква исходного текста (из верхней строки таблицы) заменяется на соответствующую букву из нижней строки. Таким образом, в результате шифрования сообщения «БОЛЬШАЯ ПЕРЕМЕНА» будет получен шифртекст «ДСОЯЫГВТЗУЗПЗРГ».

1.2 Практическая часть работы

Зашифруйте сообщение «НАСТОЯЩИЙ ДРУГ С ТОБОЙ, КОГДА ТЫ НЕ ПРАВ. КОГДА ТЫ ПРАВ, ВСЯКИЙ БУДЕТ С ТОБОЙ»(Марк Твен), используя систему Цезаря со значением ключа соответствующим номеру вашего варианта по журналу учебной группы (например, номер по списку – 5; вариант –5; ключ К = 5).

1.3 Вопросы для защиты лабораторной работы № 1

1) В чем особенность шифров простой замены?

2) Чем отличаются система шифрования Цезаря и аффинная система подстановок Цезаря?

3) Какие требования предъявляются к выбору ключей для аффинной системы подстановок Цезаря?

2 Лабораторная работа № 2. Шифрование с использованием системы Вижинера

Цель работы: формирование умений шифрования с использованием системы Вижинера.

2.1 Теоретические сведения

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свой шифр простой замены. К таким шифрам относятся система Вижинера и «двойной квадрат» Уитстона. Рассмотрим систему Виженера на практике.

Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены описывается таблицей шифрования, называемой таблицей Вижинера (Приложение А).

Таблица Вижинера имеет два входа:

- верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;

- крайний левый столбец ключа.

Последовательность ключей получают из порядковых номеров в алфавите букв ключевого слова (начиная с 0). При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово или фразу. Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Рассмотрим пример шифрования сообщения «БОЛЬШАЯ ПЕРЕМЕНА». Ключевое слово – «РАБОТА». Ход шифрования и его результат отображеныв таблице 1.

Таблица 1 – Пример шифрования сообщения

Сообщение	Б	О	Л	Ь	Ш	А	Я		П	Е	Р	Е	М	Е	Н	А
Ключевое слово	**р**	**а**	**б**	**о**	**т**	**а**	**р**		**а**	**б**	**о**	**т**	**а**	**р**	**а**	**б**
Ключи	16	0	1	14	18	0	16		0	1	14	18	0	16	0	1
Шифртекст	с	о	м	к	к	а	п		п	ж	ю	ч	м	х	н	б

2.2 Практическая часть работы

Используя систему Вижинера, зашифруйте сообщения по вариантам, приведенным в таблице 2. Текст сообщения и ключевое слово должны соответствовать вашему варианту по журналу учебной группы (например, если номер по списку 3, значит вариант – 3).

Таблица 2 – Задание для практической работы № 2

№ варианта	Сообщение	Ключевое слово
1	2	3
1	За пару секунд компьютер успевает сделать ошибку таких размеров, что сотни людей трудятся над ней месяцами	РАДОСТЬ
2	Первые криптографические системы были изобретены в глубокой древности, но не перестали развиваться в наши дни	УСПЕХ
3	Первые каналы связи были очень простыми, их организовывали с помощью надежных курьеров	ЛЕТО
4	Процесс преобразования открытого текста с целью сделать непонятным его смысл для посторонних называется шифрованием	УДАЧА

Продолжение таблицы 2

1	2	3
5	Знания бывают двоякого рода: либо мы что-нибудь знаем, либо мы знаем, где найти сведения об этом	ПРАЗДНИК
6	Параметр, с помощью которого выбирается отдельное используемое преобразование, называется криптографическим ключом	МЫШКА
7	Расшифрование – процесс извлечения открытого текста из криптограммы при условии знания ключа	КСЕРОКС
8	Каждое криптографическое преобразование однозначно определяется ключом и описывается некоторым криптографическим алгоритмом	КАНИКУЛЫ
9	Криптосистема является криптостойкой, если предпринятые криптоаналитические атаки не достигают	КОМПЬЮТЕР
10	Ключ передается отправителю и получателю сообщения таким образом, что его невозможно перехватить	РУЧКА
11	Весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитикам противника	КИНОТЕАТР
12	Криптосистема, реализующая семейство криптографических преобразований, обычно является открытой системой	ФИАЛКА
13	Целью криптоанализа может быть как получение открытого текста, так и определение секретного компонента шифра - ключа	ПРОГРАММА
14	С развитием компьютерных технологий и вычислительной техники усложнились и методы шифрования	РАБОТА

Продолжение таблицы 2

1	2	3
15	Системы шифрования дисковых данных могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков	ВЕСНА
16	При обмене данными по сетям возникает проблема установления подлинности авторов созданного сообщения	СОЛНЦЕ
17	В системе прозрачного шифрования преобразования осуществляются незаметно для пользователя	ЖИЗНЬ
18	Решетка Кардано – это прямоугольная или квадратная карточка с четным числом строк и столбцов	ПЕРЕМЕНА
19	Целью криптоанализа может быть как получение открытого текста, так и определение секретного компонента шифра - ключа	ПИСЬМО
20	В качестве нормативного алфавита может применяться, например, русский алфавит, исключая некоторые буквы, дополненный пробелом	КАРАНДАШ
21	Криптоаналитическая атака против шифра простой замены начинается с подсчета частот появления символов	ЛЕКЦИЯ
22	В процессе шифрования первым ключом шифруется первый символ открытого текста, вторым ключом – второй	МОНИТОР
23	С развитием компьютерных технологий и вычислительной техники усложнились и методы шифрования	СМЫСЛ
24	Системы второго типа являются утилитами шифрования, которые необходимо специально вызывать	ПАМЯТЬ

Продолжение таблицы 2

1	2	3
25	В случае канального шифрования защищается информация, передаваемая по каналу связи, включая служебную	РАБОТА
26	Вирусы, находящиеся после активации в оперативной памяти компьютера и контролируют доступ к его ресурсам	МАШИНА
27	Вирусы, которые выполняются только в момент запуска зараженной программы, называют транзитными	СВЕДЕНИЯ
28	Копирование вируса в середину файла может произойти в результате ошибки вируса – файл может быть необратимо испорчен	КНИГА
29	Перезаписывающие вирусы записывают свой код вместо кода заражаемого файла, уничтожая его содержимое	ПРАВДА
30	Системы шифрования дисковых данных могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков	ПРИНТЕР

2.3 Вопросы для защиты лабораторной работы № 2

1) Чем шифры простой замены отличаются от шифров сложной замены?

2) Какой ключ используется в системе Вижинера?

3) В чем заключается алгоритм шифрования текста с использованием системы Вижинера?

3 Лабораторная работа № 3. Криптоанализ шифров простой замены

Цель работы: научиться расшифровывать сообщения методом анализа числовых показателей с помощью Гистограммы частот появления символов русского алфавита в зашифрованном сообщении.

3.1 Теоретическиесведения

Шифры простой замены обладают важным свойством: они не нарушают статистических характеристик языка исходного текста. Поэтому криптоанализ шифра простой замены может основываться на использовании статистических закономерностей естественного языка.

Шифры простой замены легко вскрываются с помощью частотного анализа – метода, основанного на анализе частот появления различных букв (чисел, символов) в шифротексте. При этом наиболее часто встречающиеся буквы криптограммы заменяются наиболее вероятными символами нормативного алфавита.

Причинами осуществления успешных атак на алгоритмы шифрования являются:

- статистическая структура исторически сложившихся языков. Существуют определенные символы или их комбинации, наиболее часто встречающиеся в естественной речи (например, в русском языке чаще всего встречается бука «о», затем «е», «а», «и»);

- наличие вероятных слов.Это слова или выражения, появление которых можно ожидать в перехваченном сообщении (например, «что», «как», «его», «все», «это», «на», «по», «от», «до» и т.д.).

Можно также проследить наличие в тексте большого числа повторений отдельных фрагментов текста:

- корней;

- окончаний;

- суффиксов;

- слов;

- фраз.

Криптоаналитическая атака против шифра простой замены начинается с подсчета частот появления символов: определяется число появлений каждой буквы в шифротексте.

Затем полученное распределение частот букв в шифротексте сравнивается с распределением частот букв в нормативном алфавите (рисунок 2).

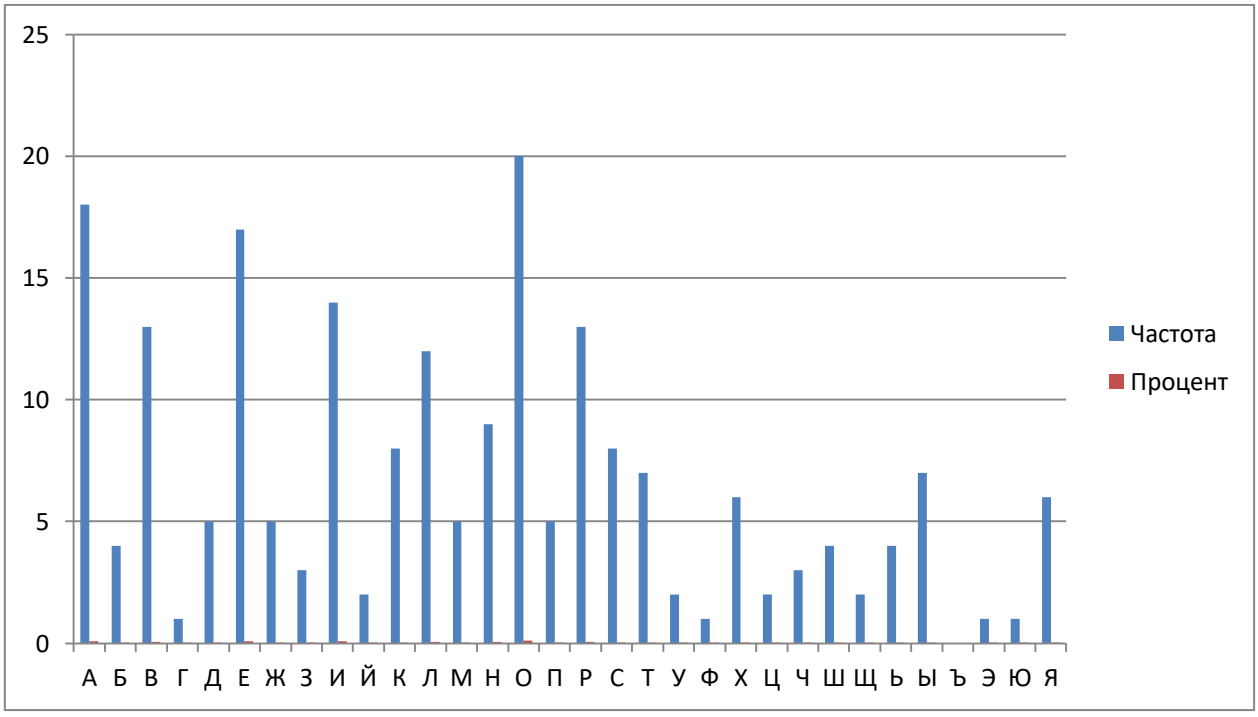


Рисунок 2– Распределение частот букв в нормативном алфавите

Для каждого языка существуют частотные таблицы символов, которые можно найти, например, в орфографических словарях.

Частоты появления символов в конкретном тексте могут отличаться (и существенно!) от стандартных (усредненных). Эти отличия могут проявиться

тем сильнее, чем короче сообщение. Поэтому частотный анализ коротких сообщений иногда бывает весьма затруднителен.

В длинных текстах (более 120 символов) частота появления букв будет приближаться к стандартной, хотя это происходит не всегда.

Поскольку частотное распределение конкретного текста может точно не совпадать с распределениями, указанными в частотной таблице, обычно приходится проверять несколько гипотез о соответствии букв шифротекста и букв открытого текста.

Если в результате проверки начинают проявляться осмысленные фрагменты текста, гипотеза признается верной, угаданные буквы подставляются в текст и производится подбор остальных букв.

3.2 Практическая часть работы

Предположим, что имеется криптограмма, полученная шифром табличной замены (рисунок 2). Символами шифр-алфавита являются двузначные числа. В тексте рассматриваемой криптограммы для простоты восприятия сохранены знаки препинания и пробелы между словами.

Требуется определить:

- исходный текст (заполнив таблицу, представленную на рисунке 3);
- ключ шифра (таблицу замен, представленную на рисунке 4).

Рисунок 3 – Криптограмма для дешифрования

Символ	11	14	16	18	19	20	22	24	25	30	34	37	39	45
Буква														

Символ	46	49	52	55	58	62	67	71	73	85	89	90	96
Буква													

Рисунок 4 – Таблица замен

Ход работы:

1) подсчитаем частоты появления символов криптограммы на рисунке 3;

2) выясним часто встречающиеся символы;

3) сопоставим их с частотами букв русского языка (рисунок 2);

4) назначим чаще всего встречающемуся номеру самую распространенную букву (скорее всего символу 11 соответствует буква «о»);

5) обратим внимание на слово в шестой строке, записанное через дефис. Предположим, что после дефиса, скорее всего, может стоять частица «то». Тогда символу 20 соответствует буква «т» (не забываем каждый найденный

символ записывать в таблицу символов, чтобы не пропустить отгаданный символ);

6) продолжаем работать с частью слова, стоящую до дефиса в шестой строке. Два символа в этом слове повторяются (34), имеются также наиболее часто встречающиеся символы 16 и 14, которые, скорее всего, являются гласными;

7) можно предположить, что часть слова, стоящая до дефиса может быть:

а) «какая» (не подходит, так как вторая и четвертая буква в предполагаемом слове должны быть одинаковыми, а в криптограмме они разные);

б) «какое» (не подходит, так как букву «о» мы уже определили, ей соответствует номер 11, такого номера в этом слове нет);

в) «какие» (можем предположить, что это слово «какие»);

8) сделаем соответствующие назначения буквам и внесем их в таблицу замен:

а) 34 – «к»;

б) 16 – «а»;

в) 18 – «и»;

г) 14 – «е»;

9) анализ текста после замены символов не выявляет никаких противоречий, так что, скорее всего, ранее были сделаны верные предположения;

10) далее обратим внимание на первое слово в первой строке. Это слово из двух букв, заканчивающееся на «а». Это могут быть слова «на» или «за», тогда первый символ 19 может быть буквами «н» или «з»;

11) обратим внимание, что третье слово в первой строке, которое имеет в середине сдвоенный символ 19. Отсюда можно сделать вывод, что символу 19 соответствует буква «н».

12) рассмотрим четвертое слово во второй строке – это слово «к_е_ко». Предположим, что это слово крепко, тогда 24 символу соответствует буква «р»,

а 45 – буква «п». Сделаем соответствующие записи в таблице замен (рисунок 4) и внесем результат в криптограмму для дешифрования (рисунок 3);

13) последнее слово шестой строки – «про_о_а» - это, скорее всего слово «провода», тогда символу 25 соответствует буква «в», а 39, соответственно, буква «д». Это не противоречит тому, что в пятой строке есть однобуквенное слово, закодированное символом 25, это может быть предлог «в».Дальнейшее вскрытие шифра не представляет труда.

Задания для самостоятельного выполнения:

Задание 1. Продолжите числовой анализ данных криптограммы, рассмотренной в п.3.2 и выясните оставшиеся буквы, делая соответствующие записи в таблице замен (рисунок 4) и внося результат в криптограмму для дешифрования (рисунок 3).

Задание 2. Используя учебник И.Н. Васильевой Криптографические методы защиты информации:

- самостоятельно подберите сообщение (не менее 200 символов);
- зашифруйте его, используя числа (повторяющиеся буквы должны быть зашифрованы одинаковыми числами);
- создайте чистую криптограмму для расшифровки и таблицу замен;
- поменяйтесь криптограммами с соседом по парте;
- расшифруйте предлагаемую криптограмму.

3.3 Вопросы для защиты лабораторной работы № 3

1) Что такое криптография?
2) Что такое криптоанализ?
3) Что такое криптограмма?
4) Назовите понятие зашифрования и расшифровывания
5) Что такое шифртекст?
6) Что такое ключ?

7) Для чего используются частотные таблицы символов?

8) Для чего применяется таблица замен при расшифровке криптограммметодом анализа числовых показателей?

4 Лабораторная работа № 4. Изучение классическихшифров замены

Цель работы: изучить процедуры шифрования и расшифровывания в шифрах Цезаря и Виженера при помощи табличного редактора MSExcel.

Теоретическая справка по изучаемой теме приведена в лабораторных работах № 1 и № 2.

4.1 Практическая часть работы

Задание 1. Зашифровать слово с помощью шифра Цезаря

Ход выполнения работы

В приложении MS Excel создать книгу, содержащую пронумерованные символы русского алфавита:

1) в первом столбце ввести номера от 0 до 32;

2) во втором столбце – символы русского алфавита по порядку;

3) в третьем столбце – снова нумерацию от 0 до 32.

Зашифровать слово «ГЛАГОЛ» с помощью шифра Цезаря с выбранным ключом, для чего:

1) ввести шифруемое слово побуквенно в ячейки первой строки (можно использовать любые незаполненные ячейки листа);

2) строкой ниже получить числовой код символов шифруемого слова с помощью функции **ВПР**:

а) первым параметром (*Искомое_значение*) функции назначить ссылку на ячейку с текущим символом шифруемого слова;

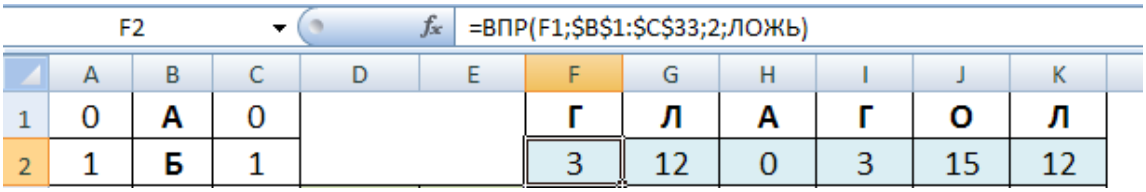
б) вторым параметром (*Таблица*) функции назначить ссылку на таблицу с алфавитом, начиная со второго столбца (столбцы B и C), ссылку на таблицу сделать абсолютной, нажав кнопку F4;

в) значение третьего параметра (*Номер_столбца*) задать равным 2 (чтобы данные брались из второго столбца выделенного на предыдущем этапе диапазона с цифрами);

г) в качестве значения четвертого параметра (*Интервальный_просмотр*) ввести слово «ЛОЖЬ» (чтобы поиск был точным).

Например: **=ВПР(F1;$B$1:$C$33;2;ЛОЖЬ)**.

Скопировать сформированную функцию **ВПР** для всех символов шифруемого слова (рисунок 5).



	A	B	C	D	E	F	G	H	I	J	K
1	0	А	0			Г	Л	А	Г	О	Л
2	1	Б	1			3	12	0	3	15	12

Рисунок 5 – Использование функции ВПР при шифровании

3) строкой ниже получить код символа криптограммы, сложив по модулю 33 (по количеству букв) полученный код текущего символа со значением ключа:

а) ввести значение ключа (согласно своему варианту);

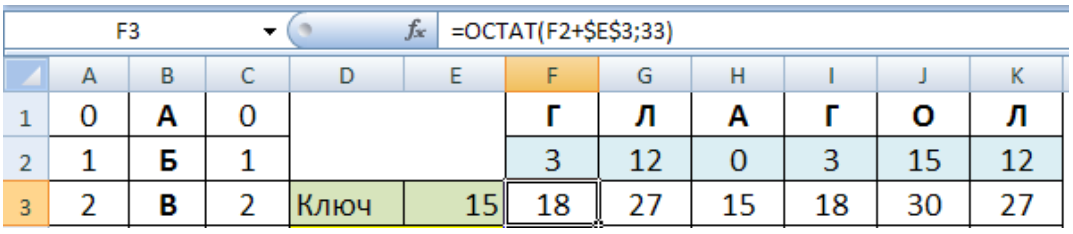
б) во второй строке под текущим символом шифруемого слова вставить функцию **ОСТАТ**;

в) в качестве первого значения первого параметра (*Число*) функции указать сумму ячейки с кодом шифруемого символа и ячейки со значением ключа (ссылку на значение ключа сделать абсолютной);

г) второй параметр (*Делитель*) задать равным 33 (по количеству букв алфавита).

Например: **=ОСТАТ(F2+$E$3;33)**.

Скопировать сформированную функцию **ОСТАТ** для всех символов шифруемого слова (рисунок 6).



	A	B	C	D	E	F	G	H	I	J	K
1	0	**А**	0			**Г**	**Л**	**А**	**Г**	**О**	**Л**
2	1	**Б**	1			3	12	0	3	15	12
3	2	**В**	2	Ключ	15	18	27	15	18	30	27

Рисунок 6 – Использование функции ОСТАТ при шифровании

4) строкой ниже с помощью функции ВПР перевести полученный код криптограммы в символьный вид:

а) в качестве значения первого параметра функции назначить ссылку на ячейку с текущим кодом криптограммы;

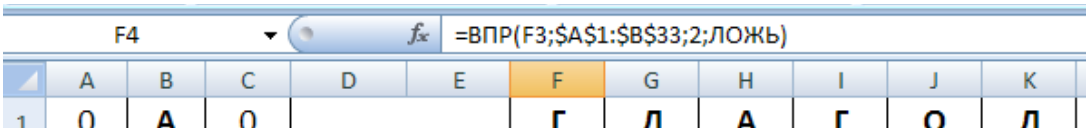
б) в качестве значения второго параметра функции назначить ссылку на таблицу с алфавитом, начиная с первого столбца (столбцы А и В), сделать ссылку на таблицу абсолютной;

в) значение третьего параметра задать равным 2;

г) в качестве значения четвертого параметра ввести слово «ЛОЖЬ».

Например: **=ВПР(F3;$A$1:$B$33;2;ЛОЖЬ)**.

Скопировать сформированную функцию **ВПР** для всех символов шифруемого слова (рисунок 7).



	A	B	C	D	E	F	G	H	I	J	K
1	0	**А**	0			**Г**	**Л**	**А**	**Г**	**О**	**Л**
2	1	**Б**	1			3	12	0	3	15	12
3	2	**В**	2	Ключ	15	18	27	15	18	30	27
4	3	**Г**	3	Шифротекст		**С**	**Ъ**	**О**	**С**	**Э**	**Ъ**
5	4	**Д**	4								

Рисунок 7–Полученная криптограмма

Проанализировать полученный текст криптограммы, обратив внимание на повторяющиеся символы.

Задание для самостоятельного выполнения: зашифровать слово КРИПТОГРАФИЯ, **в**ыбрав значение ключа шифрования в соответствии с номером своего варианта по журналу учебной группы.

Задание 2. Расшифровать криптограмму, полученную с помощью шифра Цезаря

Для того, чтобы расшифровать криптограмму выбранным ключом, необходимо:

1) ввести побуквенно текст криптограммы в ячейки одной строки;

2) строкой ниже получить числовой код символов шифруемого слова с помощью функции **ВПР**;

3) строкой ниже получить код символов расшифрованного текста, вычтя по модулю 33 (по количеству букв в алфавите) значение ключа из полученного кода текущего символа криптограммы, используя функцию **ОСТАТ** (рисунок 8);

4) строкой ниже с помощью функции **ВПР** перевести полученный код криптограммы в символьный вид.

Критерием правильности расшифровывания является получение осмысленного слова!

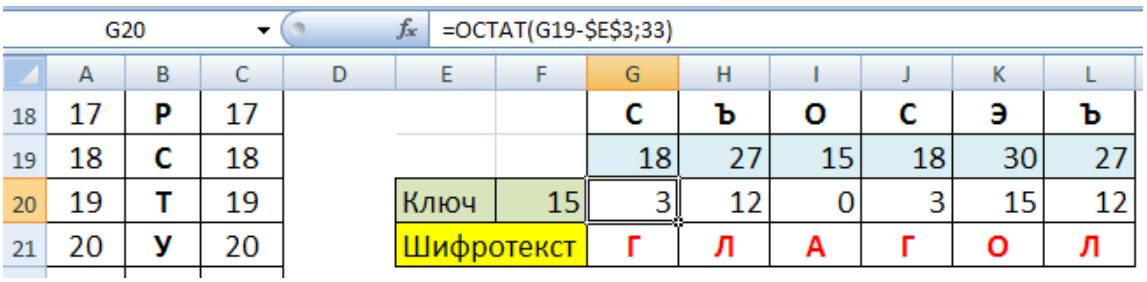


Рисунок 8–Использование функции ОСТАТ при расшифровке

Задание для самостоятельного выполнения: выбрать значение ключа шифрования и криптограмму из таблицы 3 в соответствии с номером своего варианта по журналу учебной группы.

Таблица 3 – Варианты для самостоятельного выполнения задания 2

Номер варианта	Ключ	Криптограмма	Номер варианта	Ключ	Криптограмма
1	31	пжйжимл	**17**	14	яцабндцм
2	29	жьибзеы	**18**	13	юхъыъхщ
3	28	ёазкдию	**19**	2	йвгвдв
4	27	еъкнляёц	**20**	11	тклщэк
5	26	пюжжзклх	**21**	10	фйцоъй
6	25	йлнжйкжв	**22**	9	ъцсхчу
7	24	жёгёйеё	**23**	3	ъзосезн
8	23	зящдцв	**24**	7	охтхщх
9	22	еъёъщхмх	**25**	6	чкцкжцф
10	21	егжфкэу	**26**	30	пэюрнвп
11	20	ыугьеюу	**27**	32	ётпябкы
12	19	фбгбучь	**28**	5	цжёьпе
13	18	эъгьзс	**29**	12	чяцънфвл
14	17	схухэяг	**30**	4	цифирто
15	16	яюышёшо	**31**	8	трщмуд
16	15	ачньчу	**32**	1	лбвбшпл

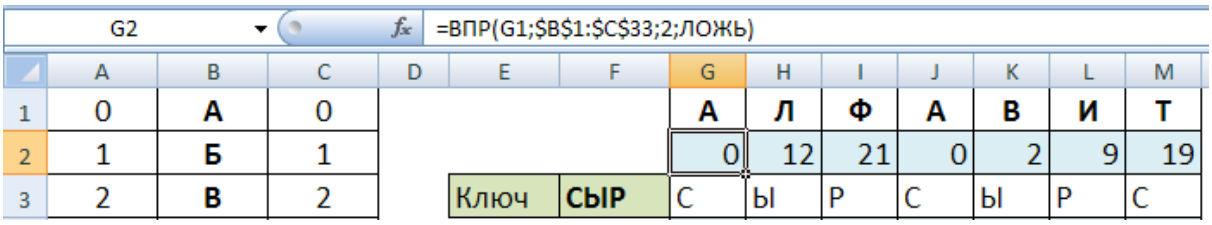
Задание 3. Зашифровать слово с помощью шифра Виженера

Зашифровать слово «АЛФАВИТ» с помощью шифра Виженера с ключевым словом «СЫР»:

- ввести побуквенно шифруемое слово в ячейки строки;

- строкой ниже получить числовой код символов шифруемого слова с помощью функции **ВПР** (рисунок 9);

- строкой ниже ввести побуквенно ключ шифра Виженера, циклические повторяя его, пока не будет достигнут конец шифруемого слова (рисунок 9);



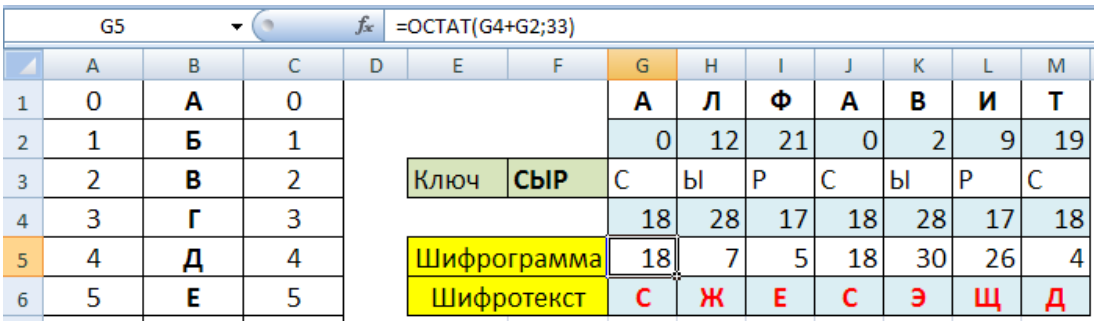
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	0	**А**	0				**А**	**Л**	**Ф**	**А**	**В**	**И**	**Т**
2	1	**Б**	1				0	12	21	0	2	9	19
3	2	**В**	2		Ключ	**СЫР**	С	Ы	Р	С	Ы	Р	С

Рисунок 9 – Использование функции ВПР при шифровании

- строкой ниже получить числовой код символов ключевой строки с помощью функции **ВПР**;

- строкой ниже получить код символа криптограммы, сложив по модулю 33 (по количеству букв в алфавите) полученный код текущего символа шифруемого слова с кодом текущего символа ключевой строки, используя функцию **ОСТАТ** (рисунок 10);

- строкой ниже с помощью функции **ВПР** перевести полученный код криптограммы в символьный вид.



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	0	**А**	0				**А**	**Л**	**Ф**	**А**	**В**	**И**	**Т**
2	1	**Б**	1				0	12	21	0	2	9	19
3	2	**В**	2		Ключ	**СЫР**	С	Ы	Р	С	Ы	Р	С
4	3	**Г**	3				18	28	17	18	28	17	18
5	4	**Д**	4		Шифрограмма		18	7	5	18	30	26	4
6	5	**Е**	5		Шифротекст		**С**	**Ж**	**Е**	**С**	**Э**	**Щ**	**Д**

Рисунок 10 – Использование функции ОСТАТ при шифровании

Задание для самостоятельного выполнения: выбрать значение **ключа шифрования** из таблицы 4 в соответствии с номером своего варианта по журналу учебной группы.

Таблица 4 – Варианты индивидуальных заданий

№ варианта	Ключ	Криптограмма	№ варианта	Ключ	Криптограмма
1	слон	гфьацючшс	**14**	стул	хбеюевбъгеп
2	клин	хфйтыщнауци	**15**	флаг	фцтцфчьргэтя
3	смех	юмчъюмчюьм	**16**	дрель	хтурюфхсрйсяцюш
4	звон	зтчвфжбцтв	**17**	цена	буюрыпанецаь
5	приз	мюнштхырър	**18**	парус	биэацврщкяюсгп
6	лист	юнэчшндгфз	**19**	скунс	юшвращшуеяаьёй
7	свет	ьрсяепнэсшнс	**20**	кот	чэащюбцчс
8	вой	фухжртёучку	**21**	право	учлрюаяийрюфсфрю
9	мир	юккячфхчф	**22**	куча	оввучшетщвшоывй
10	час	ангйаэгязая	**23**	мост	ыралсрацюбуб
11	кол	кюрцъкбчк	**24**	окно	хупэбшьрэоябрщ
12	слово	ьъьцчхрьшчсчкпэгюк	**25**	глаз	пщоксуалггнцфюь
13	клуб	бряпьюбпьюп	**26**	труд	вхдидядцыжу

Задание 4. Расшифровать криптограмму, полученную с помощью шифра Виженера

Расшифровать криптограмму выбранным ключом:

- ввести текст криптограммы побуквенно в ячейки строки отформатированной области;

- строкой ниже получить числовой код символов шифруемого слова с помощью функции **ВПР**;

- строкой ниже сформировать ключевую строку;

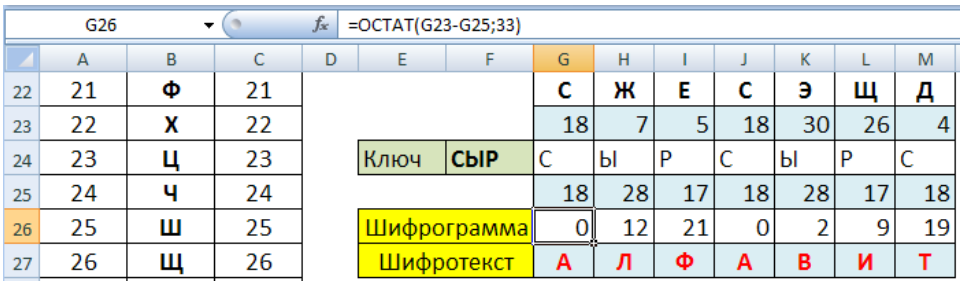
- строкой ниже получить числовой код символов ключевой строки с помощью функции **ВПР**;

- строкой ниже получить код символа открытого текста, вычтя по модулю 33 (по количеству букв в алфавите) код текущего символа ключевой строки из

кода текущего символа криптограммы, используя функцию ОСТАТ (рисунок 11);

- строкой ниже с помощью функции ВПР перевести полученный код криптограммы в символьный вид.

Критерием правильности расшифровывания является получение осмысленного слова!!!



	A	B	C	D	E	F	G	H	I	J	K	L	M
22	21	Ф	21				С	Ж	Е	С	Э	Щ	Д
23	22	Х	22				18	7	5	18	30	26	4
24	23	Ц	23		Ключ	СЫР	С	Ы	Р	С	Ы	Р	С
25	24	Ч	24				18	28	17	18	28	17	18
26	25	Ш	25		Шифрограмма		0	12	21	0	2	9	19
27	26	Щ	26		Шифротекст		А	Л	Ф	А	В	И	Т

Рисунок 11 – Использование функции ОСТАТ при расшифровке

Задание для самостоятельного выполнения: выбрать значение **ключа шифрования и криптограмму** из таблицы 4 в соответствии с номером своего варианта по журналу учебной группы, расшифровать криптограмму.

Обобщите знания, полученные в результате выполнения лабораторных работ № 2 и № 4.

Сравните таблицу букв и цифр в лабораторной работе № 4 с Таблицей Виженера, используемой в лабораторной работе № 2.

Проанализируйте возможности рассмотренных функций MSExcel.

Внесите изменения в таблицу букв и цифр лабораторной работы 4, чтобы данные из лабораторной работы № 4 совпадали с данными, полученными в результате выполнения лабораторной работы № 2.

Задание для самостоятельного выполнения:

Зашифруйте сообщение из таблицы 2, используя функций MSExcel.

Результат выполнения лабораторных работ № 2 и № 4 должен быть одинаковым!

4.2 Вопросы для защиты лабораторной работы № 4

1) Что такое криптостойкость?

2) Какие существуют требования к криптосистемам?

3) Какие существуют методы криптографического преобразования информации?

4) Какие существуют методы шифрования?

5) Что такое криптографический алгоритм?

5 Контрольные вопросы и задания по разделу

1) Приведите классификацию классических шифров по типу преобразования

2) В чем заключается криптографическое преобразование в шифрах замены?

3) В чем заключается криптографическое преобразование в шифрах перестановки?

4) Приведите примеры шифров простой и сложной замены

5) Приведите классификацию шифров по размеру преобразуемой информации

6) Сколько различных вариантов ключа имеет шифрующая система Цезаря?

7) На каких принципах строится криптоанализ шифров простой замены?

8) На каких принципах строится криптоанализ табличной перестановки?

9) На каких принципах строится криптоанализ шифра Виженера?

10) Каковы основные этапы криптоанализа шифра Виженера?

11) Почему был взломан шифр «Энигмы»?

6 Задачи по разделу

При выполнении задач предполагается, что буквы русского алфавита закодированы числами от 0 до 32.

Задание 1. Определить ключ шифра Цезаря, если известны пары «открытый текст – шифротекст»:

1) апельсин – сацэнгья;

2) засада – цоаото;

3) синица – жюгюлх;

4) ягода – дзуне;

5) лисица – гананч;

6) принтер–тулрхзу;

7) винчестер–ёмсыихциф;

8) клавиатура–ыьртщргдбр;

9) проектор–уфтиоцтф;

10) монитор –эяющгяб.

Задание 2. Определить ключ шифрования и дешифровать сообщение, полученное шифром Цезаря:

1) арутуьчн;

2) дьюка;

3) деаэц;

9) лдотс;

5) аратз;

6) сдытр;

7) пюынг;

8) омпыж;

9) ькъщн;

10) жсусёг.

Задание 3. Определить ключевое слово шифра Виженера, если известны пары «Открытый текст – шифртекст»:

1) принтер – ярйыдеа;
2) винчестер – оивжуююее;
3) клавиатура – мыеозввшья;
4) проектор – юхюкцчыл;
5) монитор – цьъьчак;
6) ноутбук – юудгйты;
7) лестница - ьквгхзз;
8) архитектор – мюацдуфюьы;
9) тротуар – гшщтдиы;
10) парабола – ыофаньпа.

7 Тестовые задания

1) Криптография – это наука о методах:
   а) кодирования информации;
   б) и алгоритмах шифрования;
   в) вскрытия шифров;
2) Предметом криптоанализа являются методы:
   а) имитозащиты сообщений;
   б) шифрования данных;
   в) вскрытия шифров;
3) Криптографическое преобразование информации – взаимно-однозначное математическое преобразование, зависящее от:
   а) длины сообщения;
   б) ключа;
   в) исходного текста;
4) Криптограммой называется:
   а) результат шифрования;

б) шифрующая система;

в) секретный параметр шифра;

5) Процесс извлечения открытого текста из криптограммы при условии значения ключа называется:

а) расшифрованием;

б) дешифрованием;

в) зашифрованием;

6) Стеганография – это наука о методах:

а) шифрования при условии секретности алгоритма шифра;

б) скрытия факта передачи секретного сообщения;

в) дешифрования сообщения без знания ключа;

7) Имитозащита – это защита системы секретной связи от:

а) вскрытия шифра;

б) перехвата сообщений;

в) навязывания ложных сообщений;

8) Шифры, осуществляющие преобразование информации порциями фиксированной длины, составленными из подряд идущих символов сообщения, называются:

а) блочными;

б) потоковыми;

в) гаммированием;

9) Все криптографические преобразования могут быть ведены к операциям двух базовых типов:

а) циклические сдвиги и перестановки;

б) замены и перестановки;

в) замены и циклические сдвиги;

10) Шифром замены являются:

а) «скитала»;

б) «квадрат Полибия»;

в) «решетка Кардано»;

11) Перестановочным шифром является:

а) шифр Цезаря;

б) шифр Виженера;

в) «решетка Кардано»;

12) Шифром сложной замены является:

а) шифр Цезаря;

б) шифр Виженера;

в) омофонический шифр;

13) Шифры сложной замены являются:

а) одноалфавитными;

б) многоалфавитными;

в) композиционными;

14) Блочными являются классические шифры:

а) простой замены;

б) сложной замены;

в) перестановки;

15) Криптография – это наука о методах:

а) кодирования информации;

б) и алгоритмах шифрования;

в) вскрытия шифров;

16) Криптосистема «Энигмы» является шифром:

а) простой замены;

б) сложной замены;

в) перестановки.

Список использованных источников

1 Тетерукова, Н.А. Защита компьютерной информации: лабораторный практикум / Н.А. Тетерукова, С.А. Апанасевич. – Минск: МГВРК, 2013. – 80 с. ISBN 978-985-526-198-9.

2 Казарин, О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения / О.В. Казарин, А.С. Забабурин. – М.: Юрайт, 20185. – 312 с. ISBN 978-5-9916-9043-0.

3 Васильева, И.Н. Криптографические методы защиты информации / И.Н. Васильева. – М.: Юрайт, 2018. – 349 с. ISBN 978-5-534-02883-6.

Приложение А

(справочное)

Таблица Виженера для русского алфавита

	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
0	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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
27	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
28	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
29	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
30	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
31	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