Лабораторная работа 3

Изучение классических шифров замены

Цель: изучить процедуры шифрования и расшифрования в шифрах Цезаря и Виженера.

Технология выполнения задания

Задание 1. Зашифровать слово с помощью шифра Цезаря.

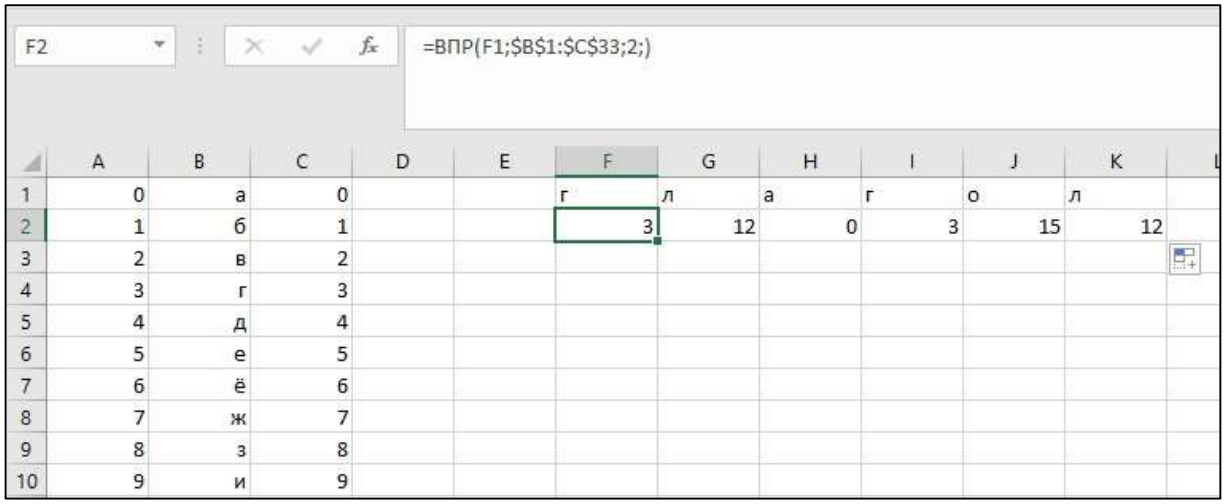
1. В приложении MS Excel создать книгу, содержащую пронумерованные символы русского алфавита: в перовом столбце ввести номера от 0 до 32, во втором – символы алфавита по порядку, в третьем – снова нумерация от 0 до 32.
2. Выбрать значение ключа равным номеру варианта (от 1 до 18).
3. Зашифровать слово «семена» с помощью шифра Цезаря с выбранным ключом:
   - ✓ ввести шифруемое слово побуквенно в ячейки первой строки отформатированной области; важно чтобы символы алфавита в таблице и символы вводимого слова были набраны в одном регистре;

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	0	а	0										
2	1	б	1										
3	2	в	2										
4	3	г	3										
5	4	д	4										
6	5	е	5										
7	6	ё	6										
8	7	ж	7										
9	8	з	8										
10	9	и	9										
11	10	й	10										
12	11	к	11										
13	12	л	12										
14	13	м	13										
15	14	н	14										
16	15	о	15										
17	16	п	16										
18	17	р	17										
19	18	с	18										
20	19	т	19										
21	20	у	20										

Рисунок 1. Пример содержания и форматирования книги «Алфавит»

   - ✓ строкой ниже получить числовой код символов шифруемого слова с помощью функции **ВПР**;
   - ✓ первым параметром (Искомое_значение) функции назначить ссылку на ячейку с текущим символом шифруемого слова

- ✓ вторым параметром (Таблица) функции назначить ссылку на таблицу с алфавитом начиная со второго столбца (столбцы 2 и 3), ссылку на таблицу сделать абсолютной нажав кнопку F4
- ✓ значение третьего параметра (Номер_столбца) задать равным 2
- ✓ в качестве значения четвертого параметра (Интервальный_просмотр) ввести слово ложь, например=**ВПР(F1;$B$1:$C$33;2;ЛОЖЬ)** скопировать функцию для всех символов шифруемого слова.

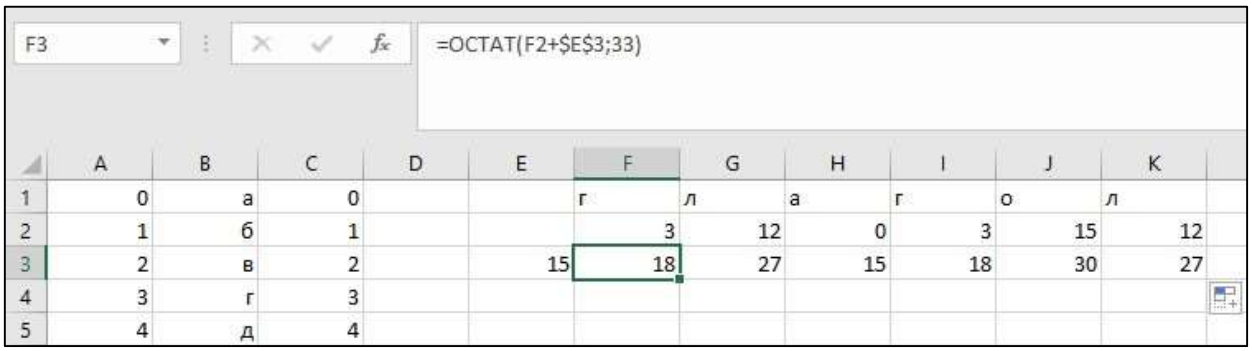


	A	B	C	D	E	F	G	H	I	J	K	L
1	0	а	0			г	л	а	г	о	л	
2	1	б	1			3	12	0	3	15	12	
3	2	в	2									
4	3	г	3									
5	4	д	4									
6	5	е	5									
7	6	ё	6									
8	7	ж	7									
9	8	з	8									
10	9	и	9									

Рисунок 2. Пример вычисления числового кода символа

- ✓ строкой ниже получить код символа криптограммы, сложив по модулю 33 полученный код текущего символа со значением ключа:
  - ввести значение ключа,
  - во второй строке под текущим символом шифруемого слова вставить функцию **ОСТАТ**
  - в качестве значения первого параметра (Число) функции указать сумму ячейки с кодом шифруемого символа и ячейки со значением ключа (ссылку на значение ключа сделать абсолютной),
  - второй параметр (Делитель) задать равным 33, например **ОСТАТ(F2+$E$3;33)**, скопировать сформированную функцию

    ОСТАТ для всех символов шифруемого слова



	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		15	18	27	15	18	30	27
4	3	г	3								
5	4	д	4								

Рисунок 3. Пример вычисления кода криптограммы, ключ равен 15

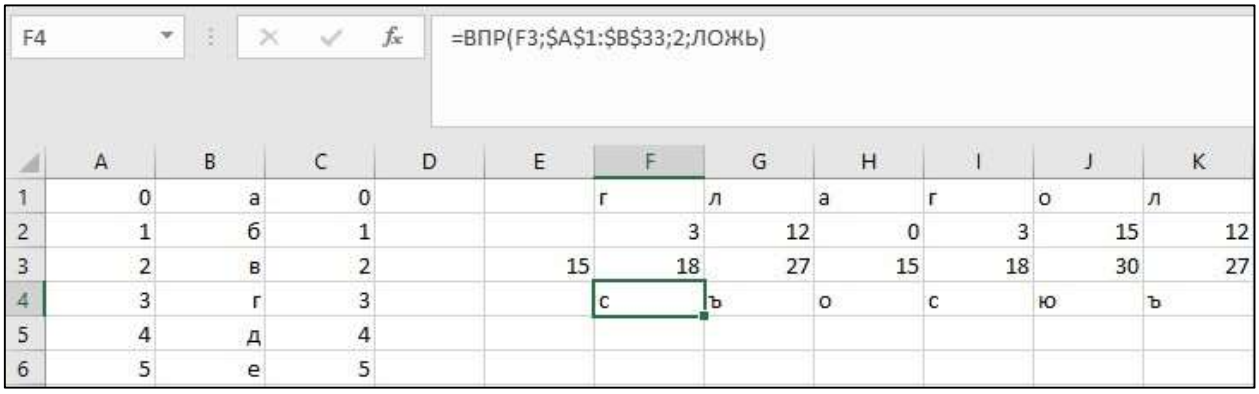
✓ строкой ниже с помощью функции ВПР перевести полученную криптограмму в символьный вид:

– в качестве значения первого параметра функции назначить ссылку на ячейку с текущим кодом криптограммы

–в качестве значения второго параметра функции назначить ссылку на таблицу с алфавитом начиная с первого столбца (столбцы 1 и 2) сделать ссылку на таблицу абсолютной

– значение третьего параметра (Номер_столбца) задать равным 2

–в качестве значения четвертого параметра (Интервальный_просмотр) ввести слово ложь, например **=ВПР(F3;$A$1:$B$33;2;ЛОЖЬ)** скопировать функцию для всех символов шифруемого слова



	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		15	18	27	15	18	30	27
4	3	г	3			с	ъ	о	с	ю	ъ
5	4	д	4								
6	5	е	5								

Рисунок 4. Пример текста, зашифрованного шифром Цезаря

✓ Проверить результат шифрования с помощью онлайн-калькулятора http://planetcalc.ru/1434/

✓ Проанализировать полученный текст криптограммы, обратив внимание на повторяющиеся символы.

Варианты задания

выбрать три на выбор

Номер варианта	Ключ	Слово
1	16	арбуз
2	27	сиквел
3	14	ивасаки
4	20	ульсан
5	21	кёнгидо
6	12	пусан
7	10	токио
8	11	сеул
9	13	лекция
10	9	руслан
11	8	линч
12	23	нетфликс
13	4	аниме
14	28	лакруа
15	30	шоколад
16	5	памело
17	2	апельсин
18	19	мандарин

Задание 2. Расшифровать криптограмму, полученную с помощью шифра Цезаря.

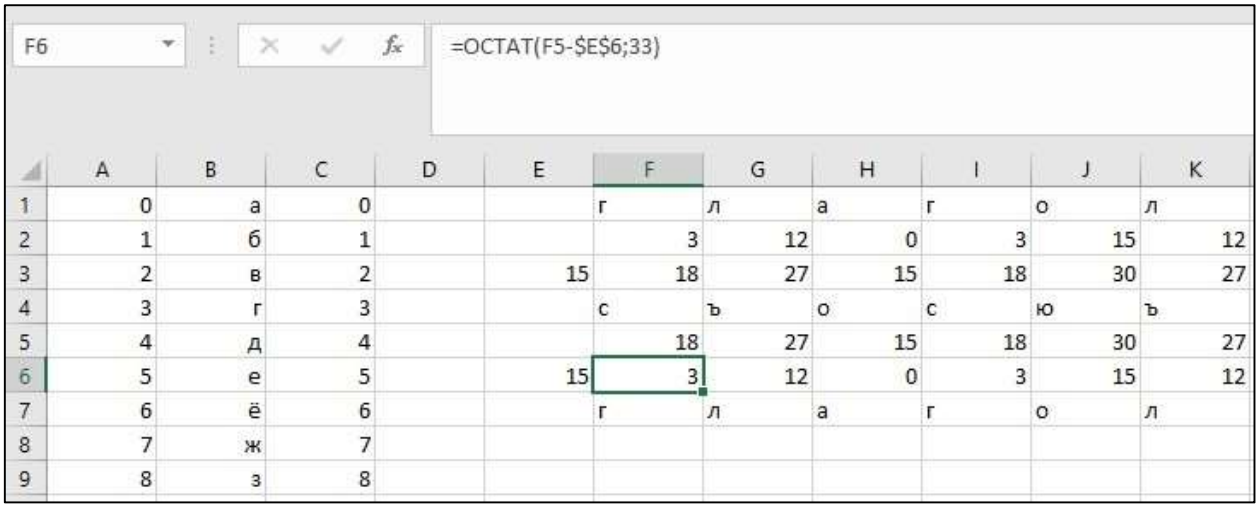
выбрать три на выбор

1. Выбрать значение ключа шифрования и криптограмму в соответствии с номером варианта

Номер варианта	Ключ	Криптограмма
1	31	п ж й ж и м л
2	29	ж ь и б з е ы
3	28	ё а з к д и ю
4	27	е ъ к н л я ё ц
5	26	п ю ж ж з к л х

6	25	й л н ж й к ж в
7	24	ж ё г ё й е ё
8	23	з я щ д ц в
9	22	е ъ ё ъ щ х м х
10	21	е г ж ф к э у
11	20	ы у г ь е ю у
12	19	ф б г б у ч ь
13	18	э ъ г ь з с
14	17	с х у х э я г
15	16	я ю ы ш ё ш о
16	15	а ч н ь ч у
17	14	я ц а б н д ц м
18	13	ю х ъ ы ъ х щ

2. Расшифровать криптограмму выбранным ключом:
   - ✓ ввести побуквенно текст криптограммы в ячейки строки отформатированной области, важно, чтобы символы алфавита в таблице и символы вводимого слова были набраны в одном регистре
   - ✓ строкой ниже получить числовой код символов шифруемого слова с помощью функции ВПР
   - ✓ строкой ниже получить код из символов расшифрованного текста, вычтя по модулю 33 значение ключа из полученного кода текущего символа криптограммы, используя функцию **ОСТАТ**



	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		15	18	27	15	18	30	27
4	3	г	3			с	ъ	о	с	ю	ъ
5	4	д	4			18	27	15	18	30	27
6	5	е	5		15	3	12	0	3	15	12
7	6	ё	6			г	л	а	г	о	л
8	7	ж	7								
9	8	з	8								

Рисунок 5. Пример вычисления кода открытого текста шифра Цезаря

- ✓ строкой ниже с помощью функции ВПР перевести полученный код криптограммы в символьный вид. Критерием правильности расшифрования является получение осмысленного слова

Задание 3. Зашифровать слово с помощью шифра Виженера.

выбрать три на выбор

1. Выбрать значение ключа шифрования в соответствии с номером варианта

Вариант задания

Номер варианта	Ключ	Криптограмма
1	слон	г ф ь а ц ю ч ш е
2	клин	х ф й т ы щ н а у ц и
3	смех	ю м ч ъ ю м ч ю ь м
4	звон	з т ч в ф ж б ц т в
5	приз	м ю н ш т х ы р ъ р
6	лист	ю н э ч ш н д г ф з
7	свет	ь р с я е п н э с ш н с
8	вой	ф у х ж р т ё у ч к у
9	мир	ю к х я ч ф х ч ф
10	час	а н г й а э г я з а я
11	кол	к ю р ц ъ к б ч к
12	слово	ь ъ ь ц ч х р ь ш ч с ч к п э г ю к
13	клуб	б р я п ь ю б п ь ю п
14	стул	х б е ю е в б ъ г е п
15	флаг	ф ц т ц ф ч ь р г э т я
16	дрель	х т у р ю ф х с р й с я ц ю ш
17	цена	б у ю р ы п а н е ц а ь
18	парус	б и э а ц в р щ к я ю с г и

2. Зашифровать слово «алфавит» с помощью Виженера с выбранным ключом:

- ✓ Ввести побуквенно шифруемое слово в ячейки строки отформатированной области; важно, чтобы символы алфавита в таблице и символы вводимого слова были набраны в одном регистре
- ✓ Строкой ниже получить числовой код символов шифруемого слова с помощью функции **ВПР**
- ✓ Строкой ниже ввести побуквенно ключ шифра Виженера, циклически повторяя его, пока не будет достигнут конец шифруемого слова

	A	B	C	D	E	F	G	H	I	J	K	L
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			с	ы	р	с	ы	р	с
4	3	г	3									
5	4	д	4									
6	5	е	5									
7	6	ё	6									
8	7	ж	7									

Рисунок 6. Пример создания ключевой строки шифра Виженера, ключевое слово «сыр»

- ✓ Строкой ниже получить числовой код символов ключевой строки с помощью функции **ВПР**
- ✓ Строкой ниже получить код символа криптограммы, сложив по модулю 33 полученный код текущего символа шифруемого слова с кодом текущего символа ключевой строки, используя функцию **ОСТАТ**

F5 =ОСТАТ(F4+F2;33)

	A	B	C	D	E	F	G	H	I	J	K	L
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			с	ы	р	с	ы	р	с
4	3	г	3			18	28	17	18	28	17	18
5	4	д	4			18	7	5	18	30	26	4
6	5	е	5			с	ж	е	с	э	щ	д
7	6	ё	6									
8	7	ж	7									

Рисунок 7. Пример вычисления кода криптограммы шифра Виженера

- ✓ Строкой ниже с помощью функции ВПР перевести полученный код криптограммы в символьный вид

- ✓ Проверить результат шифрования с помощью онлайн-калькулятора http://planetcalc.ru/2468/

Задание 4. Расшифровать криптограмму, полученную с помощью шифра Виженера

1. Выбрать значение ключа шифрования и криптограмму в соответствии с номером варианта
2. Расшифровать криптограмму выбранным ключом:

- ✓ ввести текст криптограммы побуквенно в ячейки строки отформатированной области; важно, чтобы символы алфавита в таблице и символ вводимого слова были набраны в одном регистре
- ✓ 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 код текущего символа ключевой строки из кода текущего символа криптограммы, используя функцию **ОСТАТ**
- ✓ строкой ниже с помощью функции **ВПР** перевести полученный код криптограммы в символьный вид. Критерием правильности расшифрования является получение осмысленного слова.

	A	B	C	D	E	F	G	H	I	J	K	L
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			с	ы	р	с	ы	р	с
4	3	г	3			18	28	17	18	28	17	18
5	4	д	4			18	7	5	18	30	26	4
6	5	е	5			с	ж	е	с	э	щ	д
7	6	ё	6			18	7	5	18	30	26	4
8	7	ж	7			с	ы	р	с	ы	р	с
9	8	з	8			18	28	17	18	28	17	18
10	9	и	9			0	12	21	0	2	9	19
11	10	й	10			а	л	ф	а	в	и	т
12	11	к	11									

Рисунок 8. Пример вычисления кода открытого текста шифра Виженера