Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
_____ О.В. Фомичева
«26» декабря 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.02.02 Криптографические средства защиты информации
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

для специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Методические рекомендации одобрены на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь для выполнения практических работ предназначена для организации работы на практических занятиях по МДК.02.02 «Применение криптографических средств защиты информации» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами», являющегося важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Практические занятия являются неотъемлемым этапом изучения тем 2.1 -2.5 МДК.02.02 «Применение криптографических средств защиты информации» и проводятся с целью:

формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;

обобщения, систематизации, углубления, закрепления полученных теоретических знаний;

готовности использовать теоретические знания на практике.

Практические занятия по МДК.02.02 «Применение криптографических средств защиты информации» способствуют формированию следующих общих и профессиональных компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В Рабочей тетради предлагаются к выполнению практические работы, предусмотренные рабочей программой ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлен ПМ.02.

Выполнение практических работ в рамках МДК.02.02 «Применение криптографических средств защиты информации» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» позволяет освоить комплекс работ по использованию криптографических программных средств, в Рабочей тетради представлены примеры применения программных средств криптографической защиты 2.1 -2.5 МДК.02.02 «Применение криптографических средств защиты информации».

Рабочая тетрадь для выполнения практических заданий МДК.02.02 «Применение криптографических средств защиты информации» имеет практическую направленность и значимость. Формируемые в процессе их проведения умения могут быть использованы студентами в будущей профессиональной деятельности.

80-90 % заданий направлено на выполнение, моделирование обучающимися практических видов работ, связанных с будущей профессиональной деятельностью в условиях, приближенных к реальным производственным.

Рабочая тетрадь предназначена для студентов колледжа, изучающих темы 2.1 -2.5 МДК.02.02 «Применение криптографических средств защиты информации» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и может использоваться как на учебных занятиях, которые проводятся под руководством преподавателя, так и для самостоятельного выполнения практических работ, предусмотренных рабочей программой во внеаудиторное время.

Практические занятия проводятся в учебном кабинете, не менее двух академических часов, обязательным этапом является самостоятельная деятельность студентов.

Практические занятия в соответствии с требованием ФГОС включают такой обязательный элемент, как использование персонального компьютера.

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками МДК.02.02 «Применение криптографических средств защиты информации» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и выставляются в журнале теоретического обучения.

1 ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ МДК.02.02 «ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ» ПМ.02 «ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ»

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов	
				практических занятий	в форме практической подготовки
Тема 2. Классификация шифров	З4 У6, У7	ПК 2.1-ПК 2.6 ОК 1-ОК 11	Практическая работа №1: Алгоритмизация шифра Цезаря	2	2
	З4 У6, У7	ПК 2.1-ПК 2.6 ОК 1-ОК 11	Практическая работа №2: Декодирование моноалфавитного подстановочного шифра частотным методом	2	2
Тема 3. Криптографические протоколы	З4 У6, У7	ПК 2.1-ПК 2.6 ОК 1-ОК 11	Практическая работа №3: Метод шифрования с открытым ключом RSA	2	2
	З4 У6, У7, У8	ПК 2.1-ПК 2.6 ОК 1-ОК 11	Практическая работа №4: Разработка хэш-функции	2	2
Тема 5. Стеганография	З4 У6, У7	ПК 2.1-ПК 2.6 ОК 1-ОК 11	Практическая работа №5: Анализ графических изображений на наличие скрытой информации.	2	2

2 ОПИСАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

2.1. Практическая работа № 1 «Алгоритмизация шифра Цезаря»

Задание:

Порядок выполнения:

1. Ознакомьтесь с теоретической частью практической работы.
2. Загрузите программу Microsoft Excel.
3. На первом листе электронной книги запишите в столбец А буквы русского алфавита. В столбце В – номер букв, в столбце С – опять буквы (такая запись будет необходима для использования функции ВПР).

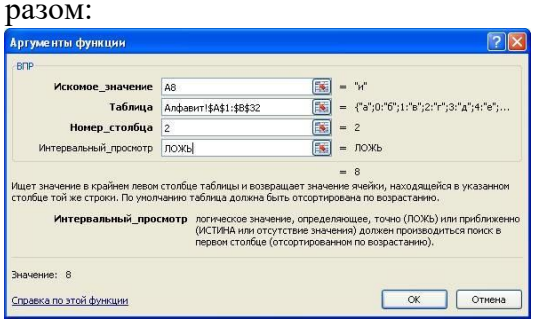
	A	B	C	D
1	а	0	а	
2	б	1	б	
3	в	2	в	
4	г	3	г	
5	д	4	д	
6	е	5	е	
7	ж	6	ж	
8	з	7	з	
9	и	8	и	
10	й	9	й	
11	к	10	к	
12	л	11	л	
13	м	12	м	
14	н	13	н	
15	о	14	о	
16	п	15	п	
17	р	16	р	
18	с	17	с	
19	т	18	т	
20	у	19	у	
21	ф	20	ф	
22	х	21	х	
23	ц	22	ц	
24	ч	23	ч	
25	ш	24	ш	
26	щ	25	щ	
27	ъ	26	ъ	
28	ы	27	ы	
29	ь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

4. Переименуйте лист1 в Алфавит.
5. На втором листе электронной книги запишите название работы, ключ и название столбцов таблицы (S – исходные символы, X – числа исходных символов, Y – пересчитанные по формуле значения, S1 – символы закрытого текста). Значение ключа можно взять любым и обязательно его значение записать в отдельную ячейку (B5). В столбец S, начиная с 8 строки, впишите фамилию и имя, каждую букву в отдельной ячейке.

	A	B	C	D	E	F	G
1				Шифр Цезаря			
2							
3	1. Зашифровывание						
4							
5	k= 5						
6							
7	S	X	Y	S1			
8	и						
9	в						
10	а						
11	н						
12	о						
13	в						
14	а						
15	н						
16	д						
17	р						
18	е						
19	й						
20							

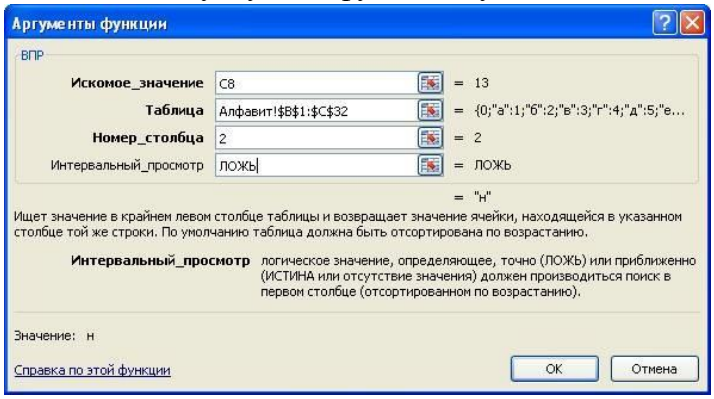
6. В столбце X должны быть числовые значения символов из столбца S. Эти значения хранятся на листе Алфавит. Чтобы получить их, можно воспользоваться функцией **ВПР** (категория – ссылки и массивы).

Встаем в ячейку B8 и вызываем функцию ВПР. Заполняем ее окно следующим образом:

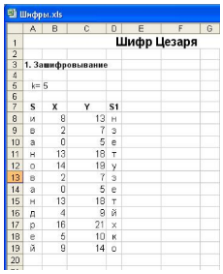


7. Растянуть формулу вниз до конца таблицы.
8. В ячейку C8 (столбец Y) записывается формула для шифрования. Исходная формула метода Цезаря имеет вид: $y_i = (x_i + k) \bmod n$. Операции mod в Excel соответствует функция **ОСТАТ(число; делитель)**. В нашем случае **число** – это $(x_i + k)$, а **делитель** – 32.

   Т.е. функция **ОСТАТ** будет иметь вид **=ОСТАТ((B8+$B$5);32)**.
9. Эту формулу необходимо растянуть вниз до конца таблицы.
10. В ячейку D8 (столбец S1) опять записываем функцию **ВПР**, которая по числу Y найдет букву. Эта функция будет выглядеть следующим образом:



11. Окончательно таблица должна выглядеть следующим образом:



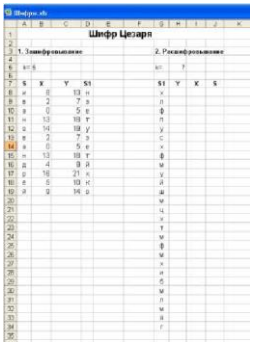
Шифр Цезаря

1. Зашифровывание

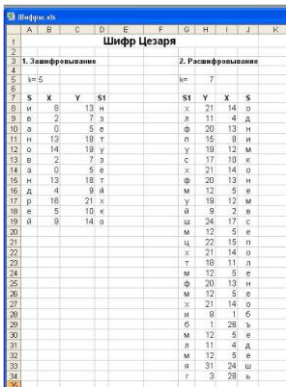
k= 5

S	X	Y	S1
и	8	13	н
в	2	7	э
а	0	5	е
н	13	18	т
о	14	19	у
в	2	7	э
а	0	5	е
н	13	18	т
д	4	9	й
р	16	21	х
е	5	10	к
й	9	14	о

12. Рядом приготовьте место для дешифрования информации. Получите у преподавателя карточку с закрытым текстом и впишите его в столбец S1 новой таблицы.



13. Проведите дешифрования текста по аналогии с зашифровыванием. Для расшифровывания (столбца X) используйте формулу $x_i = (y_i + (32-k)) \bmod 32$.



14. Запишите полученную фразу.

2.2. Практическая работа № 2 «Декодирование моноалфавитного подстановочного шифра частотным методом»

Задание:

Исходные данные:

Зашифрованный текст, перечень наиболее часто встречающихся букв в тексте, перечень наиболее часто используемых в русском языке букв.

Выходные данные: Расшифрованный текст.

Порядок выполнения:

1. Запустить на выполнение файл labw01.exe

На экране появится окно выполнения лабораторной работы (рис. 1):

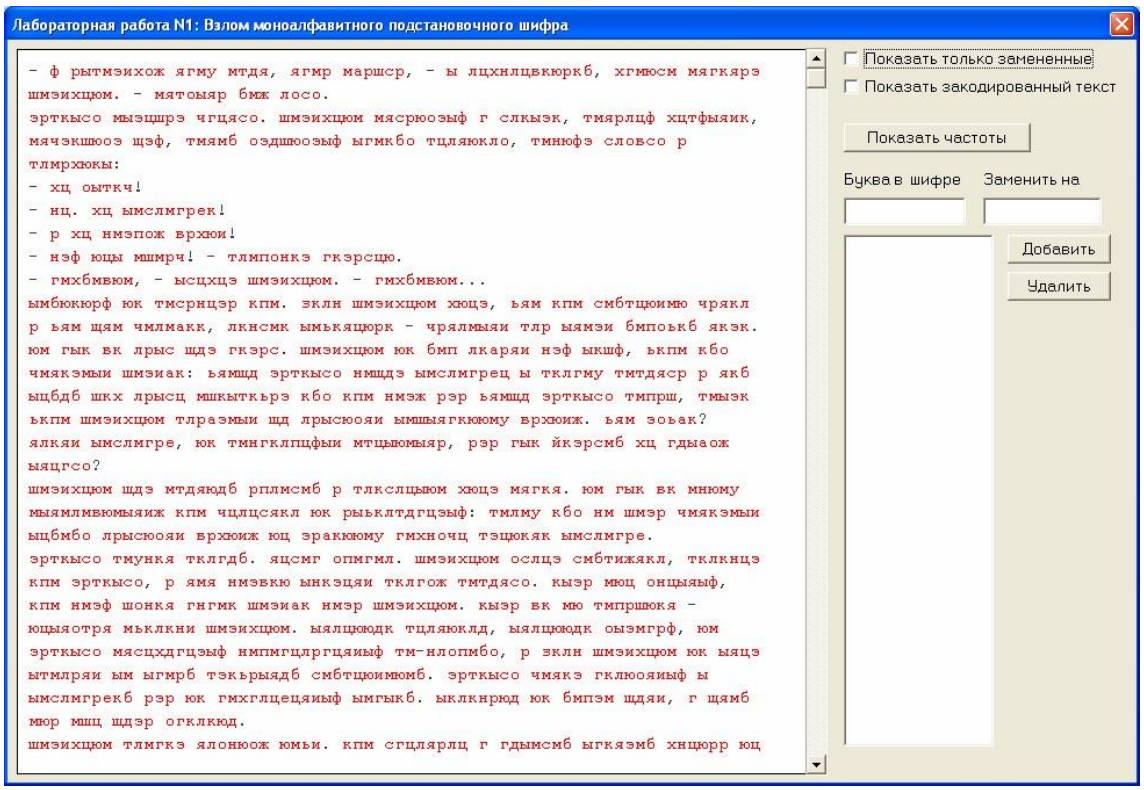


Рисунок 1. Окно выполнения лабораторной работы

В левой части окна находится зашифрованный текст (буквы, выделенные красным цветом). В процессе расшифровки расшифрованные (правильно или неправильно) буквы текста меняют цвет с красного на черный.

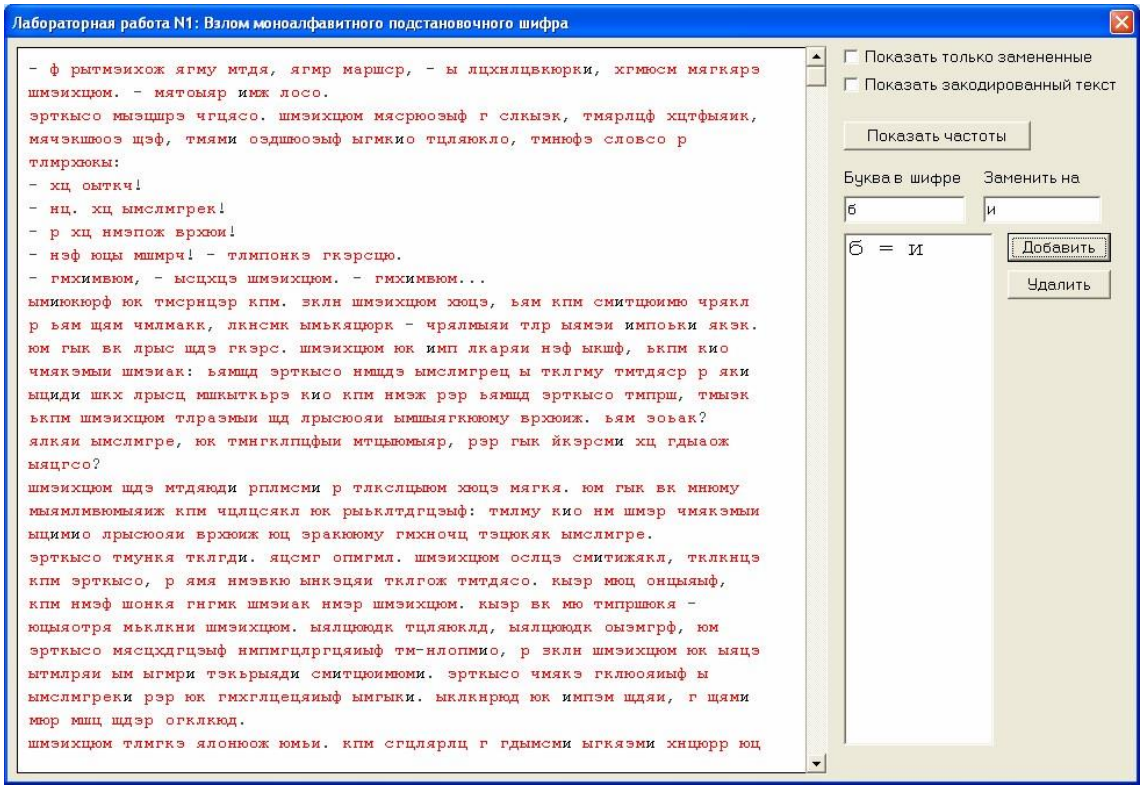


Рисунок 2. Изменения окна лабораторной работы после расшифровки одной буквы

Чтобы указать для какой-либо буквы шифра ее истинное (расшифрованное) значение, нужно в поле «Буква в шифре» указать значение буквы, например, “б”, а в поле «За-

менить на» - ее истинное значение, например, “и”, а затем нажать кнопку “Добавить“. Результат такого действия приведен на рис. 2.

На рис. 3. Приведено окно выполнения лабораторной работы после добавления расшифровок нескольких букв.

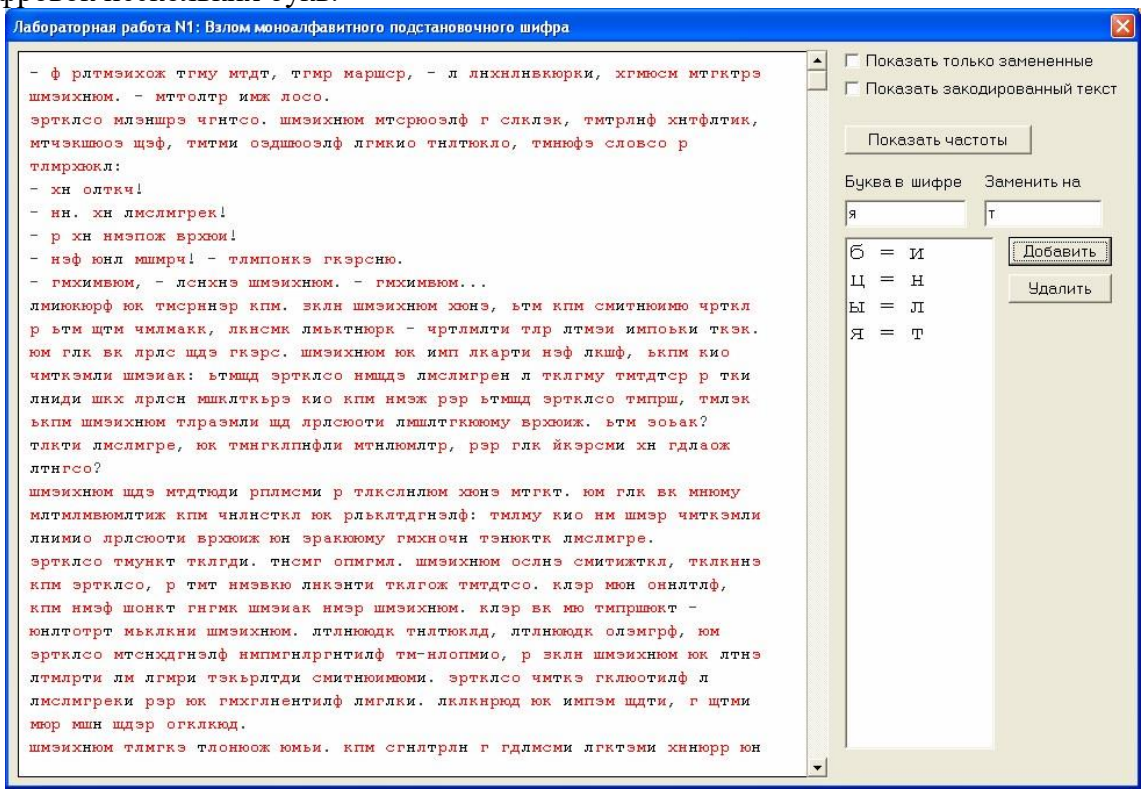


Рисунок 3. Окно лабораторной работы после расшифровки нескольких букв

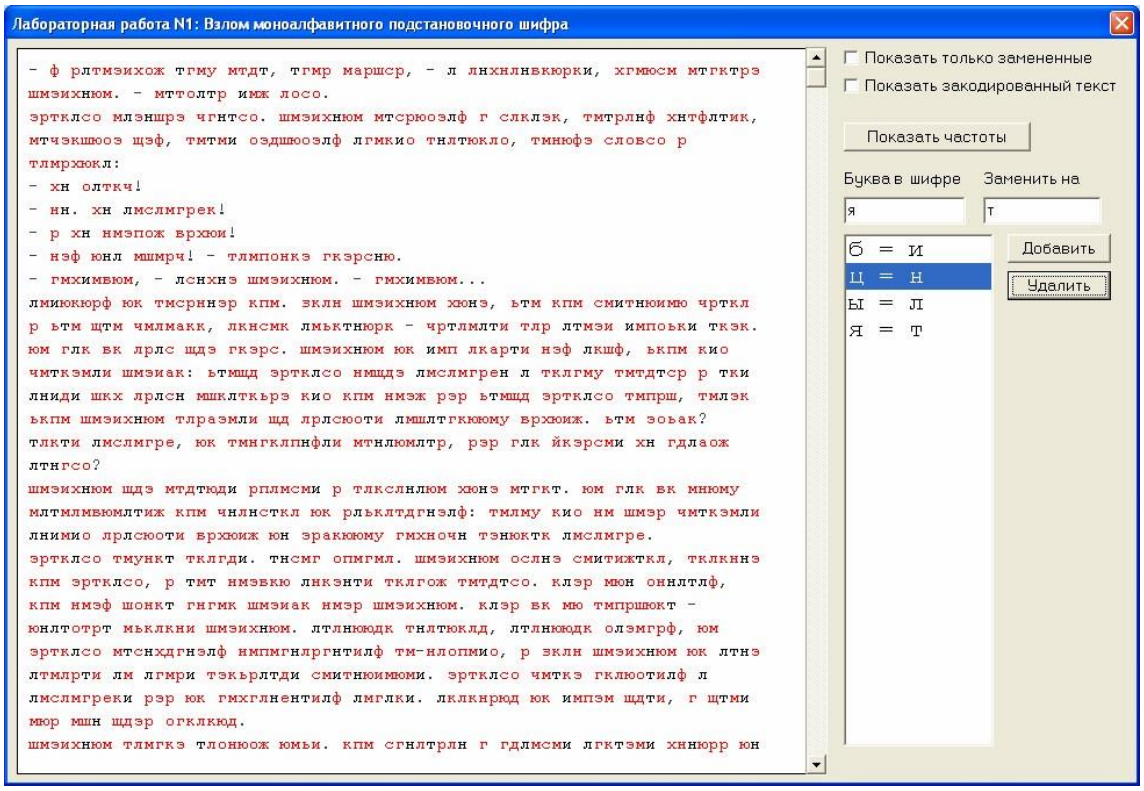


Рисунок 4. Процедура удаления ошибочно указанных расшифровок

Чтобы отменить указанную расшифровку буквы, нужно в списке расшифровок мышкой указать соответствующую пару букв и нажать кнопку «Удалить» (рис. 4).

Полоса вертикального скроллинга служит для навигации по расшифровываемому тексту.

2. Начинается частотная атака с анализа частот встречаемости букв в шифровке. Для этих целей в окне выполнения лабораторной работы предусмотрена кнопка «Показать частоты». При ее нажатии на экран выводится перечень десяти наиболее часто встречаемых букв в шифре, а также перечень букв, наиболее часто встречаемых в русском языке (рис. 5).

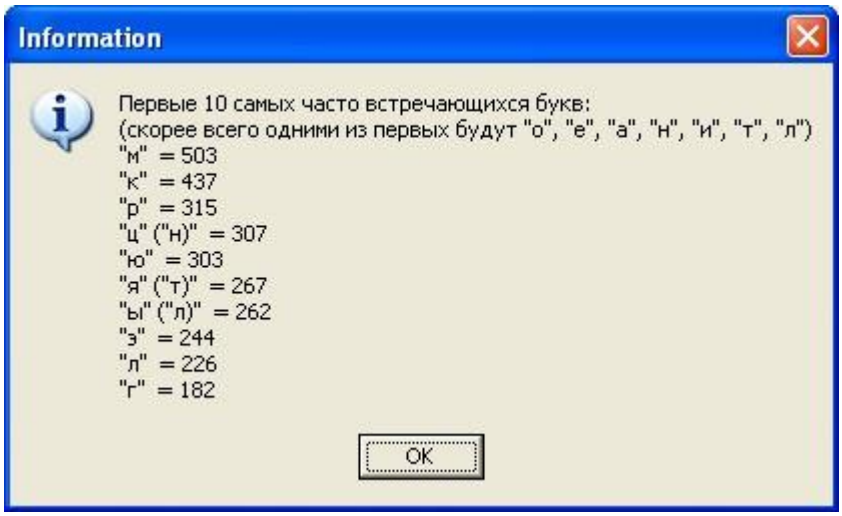


Рисунок 5. Информация о частотах встречаемости букв в шифре

Первым шагом в расшифровке текста может быть указание расшифровки для самой часто встречаемой буквы - буквы «о». Для случая, приведенного на рис. 5, указывается «о» как расшифровка буквы «м» шифра (см. рис. 6).

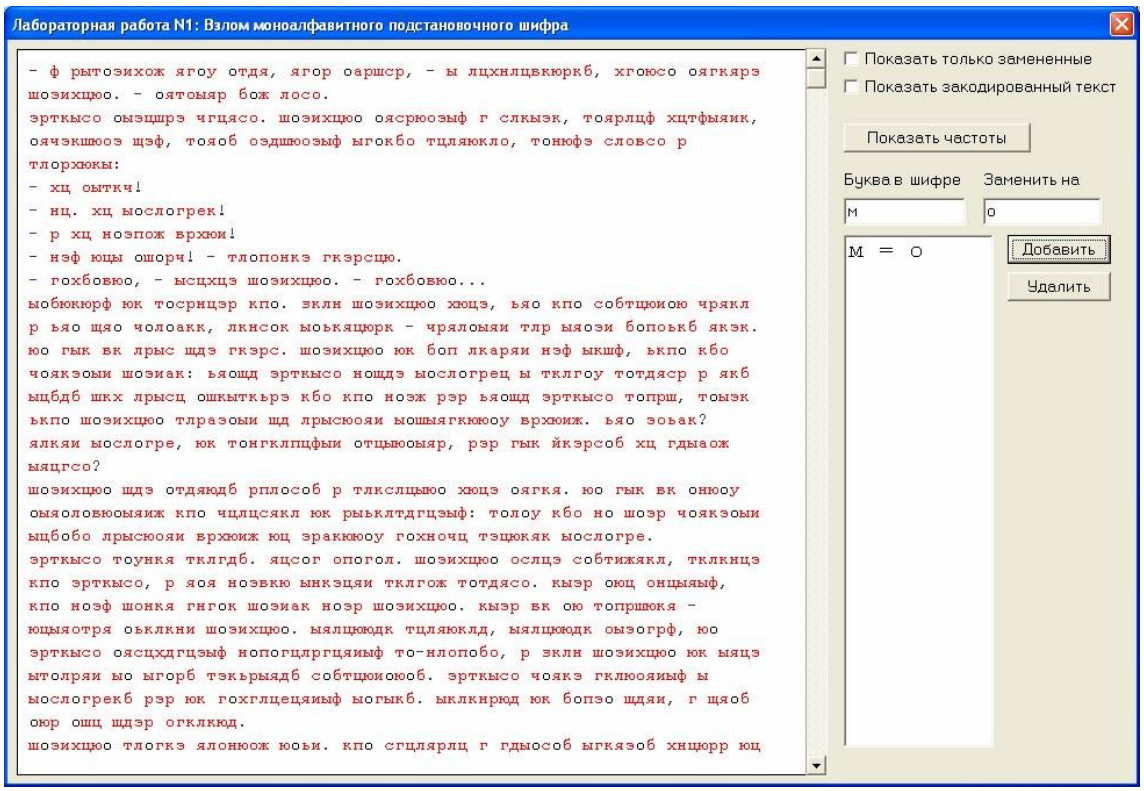


Рисунок 6. Первый шаг расшифровки - указание расшифровки буквы «о»

Следует помнить, что для конкретного текста частота встречаемости букв может быть несколько иной, чем в среднем для русского языка. Если в русском языке, например, буква «т» встречается чаще, чем буква «л», то в каком-то конкретном тексте буква «л»

вполне может встречаться чаще буквы «т». Поэтому слепо опираться на данные частотного анализа не следует.

3. В зашифрованном тексте осуществляется поиск коротких слов, зашифрованные буквы которых можно предсказать по уже расшифрованным буквам и частотной информации из рис. 5. На рис. 7. в верхней строчке есть фрагмент текста « ою », где «о» уже известно

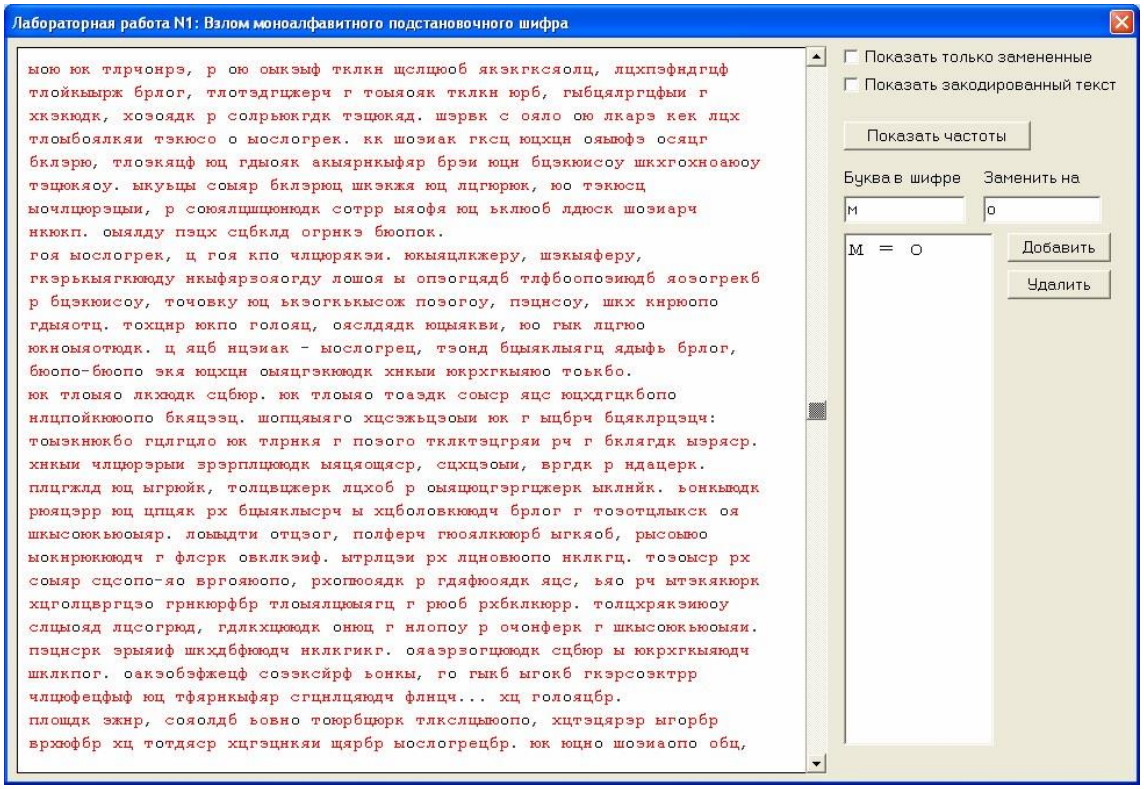


Рисунок 7. Поиск коротких слов

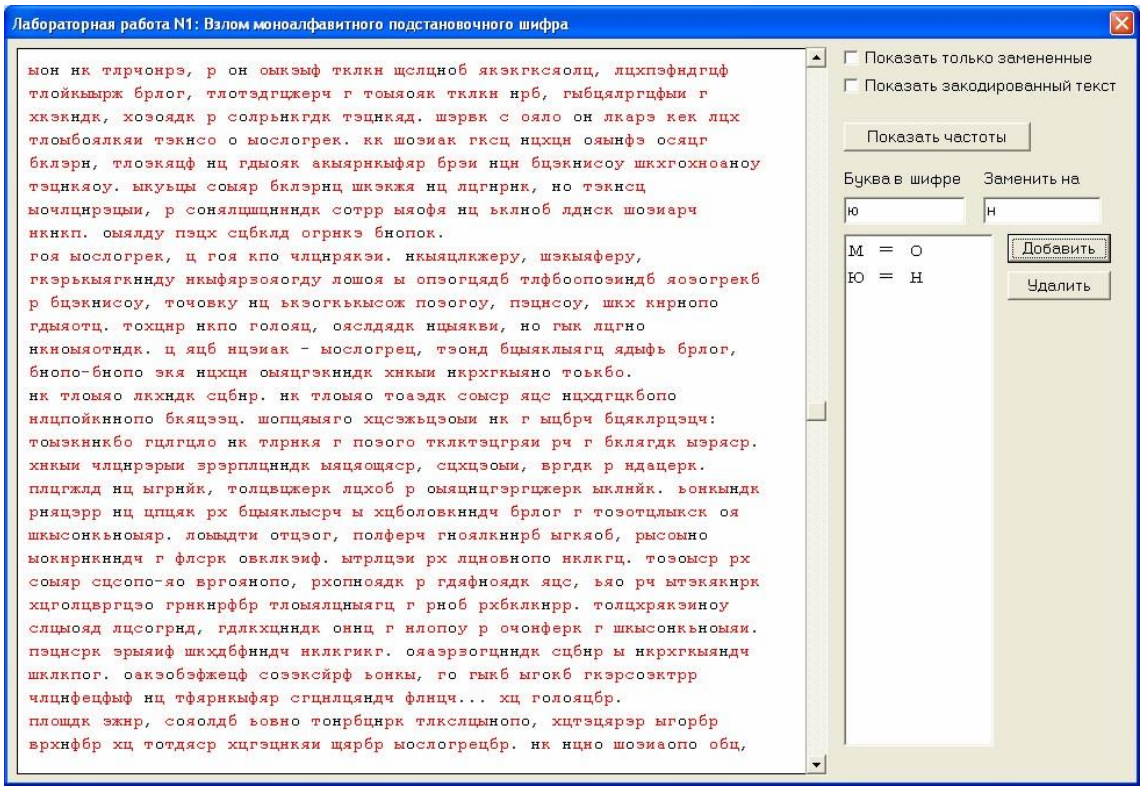


Рисунок 8. Результат расшифровки букв «о» и «н»

Этот фрагмент может быть скорее всего словом « он » В таблице частот (рис. 5) буква «ю» шифра стоит на 5-м месте, что примерно соответствует позиции буквы «н» русского языка (4-е место). Значит разумно попробовать поменять «ю» на «н». Результат приведен на рис. 8.

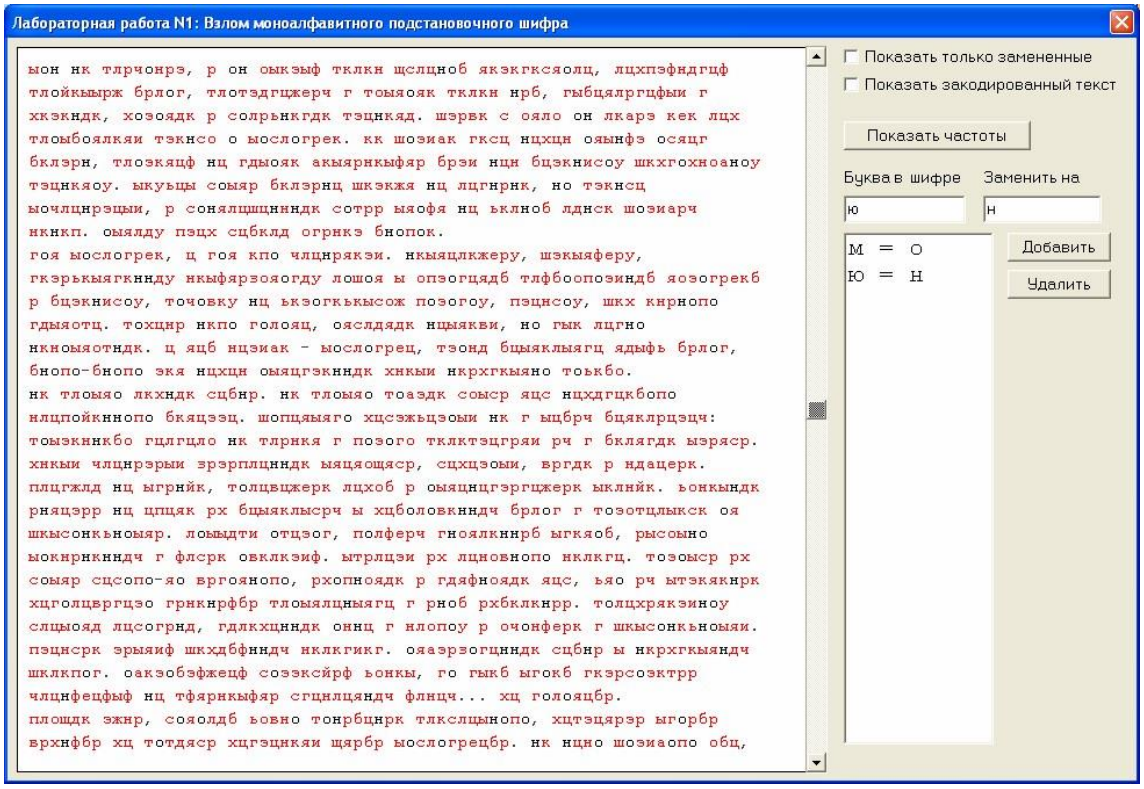


Рисунок 9. Продолжение поиска коротких понятных слов

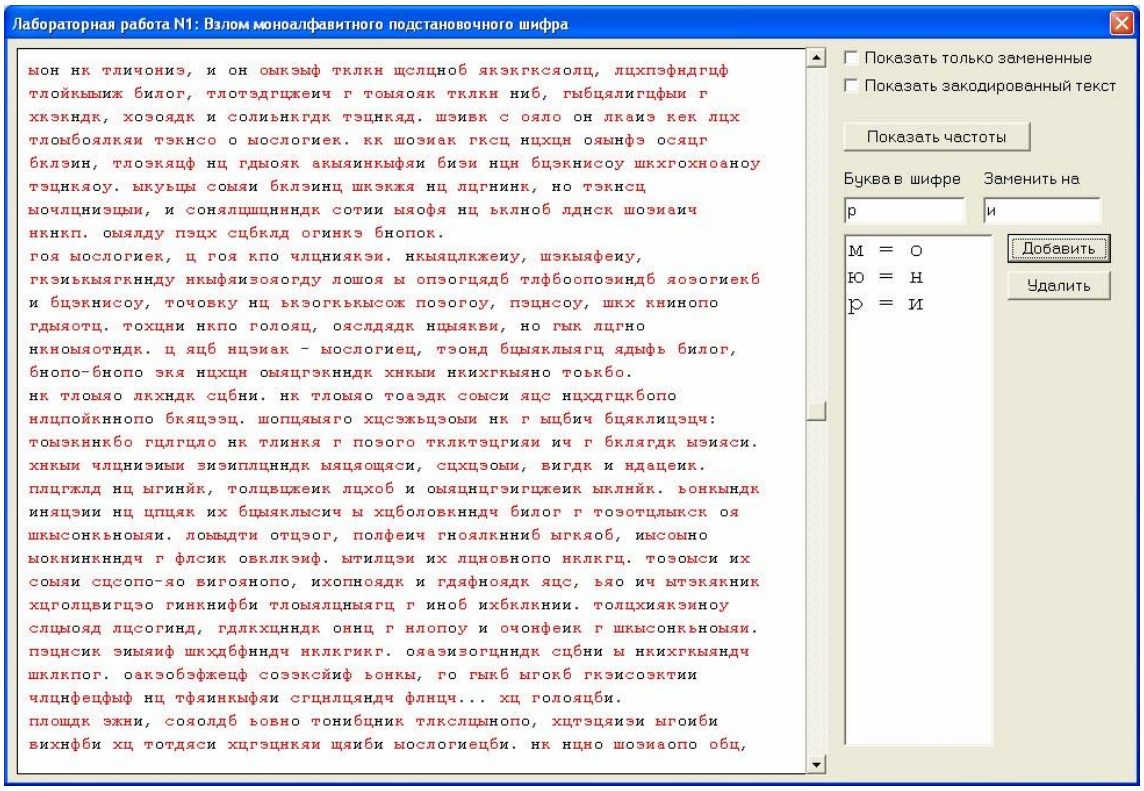


Рис. 10. Результат расшифровки букв «о», «н» и «и»

Далее повторяется поиск коротких слов, в которых можно догадаться о значении зашифрованных букв. На рис. 9 в первой и третей строках есть отдельно стоящее «р». Скорее всего это предлог «и», что согласуется и с информацией на рис. 5. Результат замены приведен на рис. 10.

На рис. 11 в первой строке обнаруживается слово из двух известных «и» и шифрованной буквы «э» между ними. Скорее всего это буква «л», образующая слово «или» (рис. 12).

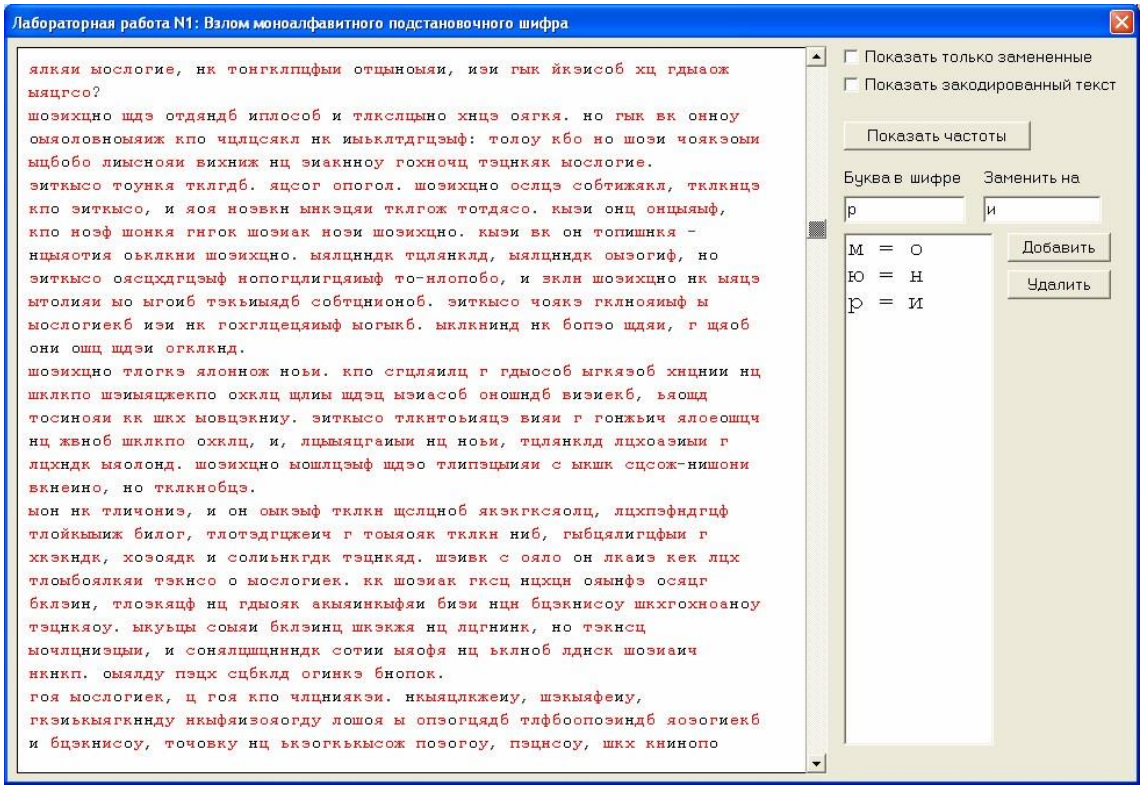


Рисунок 11. Продолжение поиска коротких понятных слов

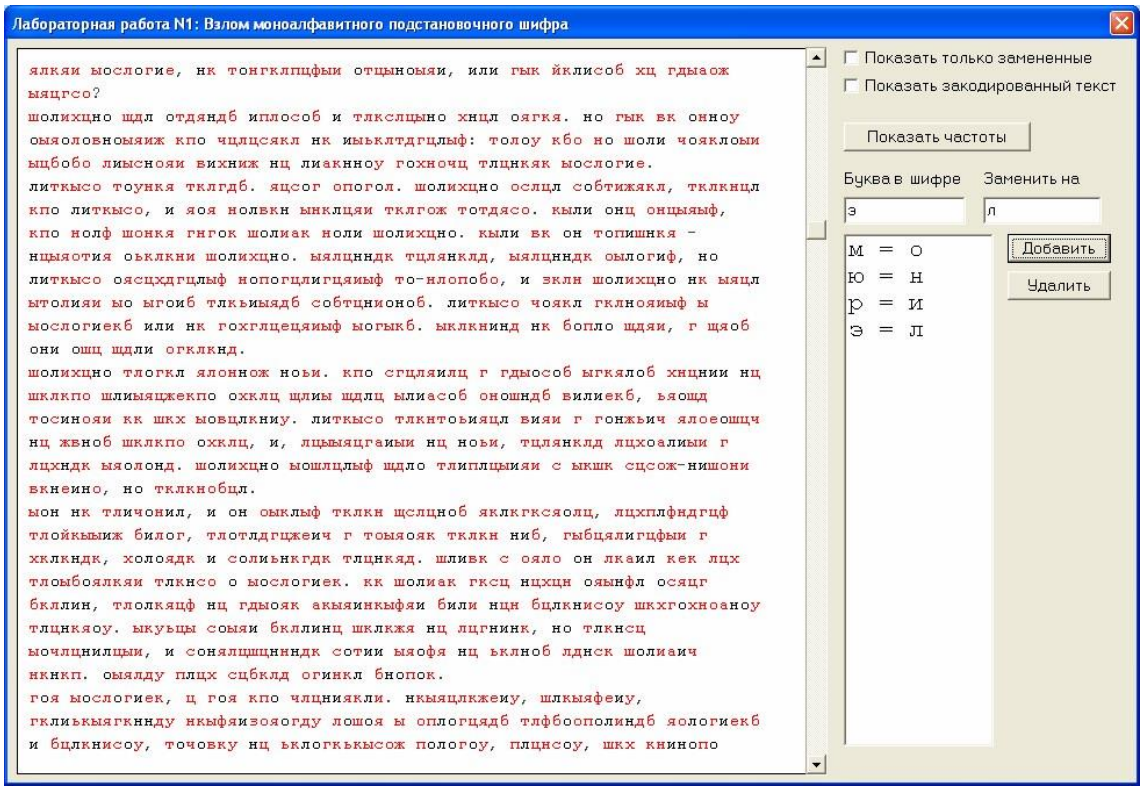


Рисунок 12. Результат расшифровки букв «о», «н», «и» и «л»

После расшифровки аналогичным образом букв «к» на «е», «ц» на «а» и «я» на «т» окно выполнения лабораторной работы приобретает следующий вид (рис. 13):

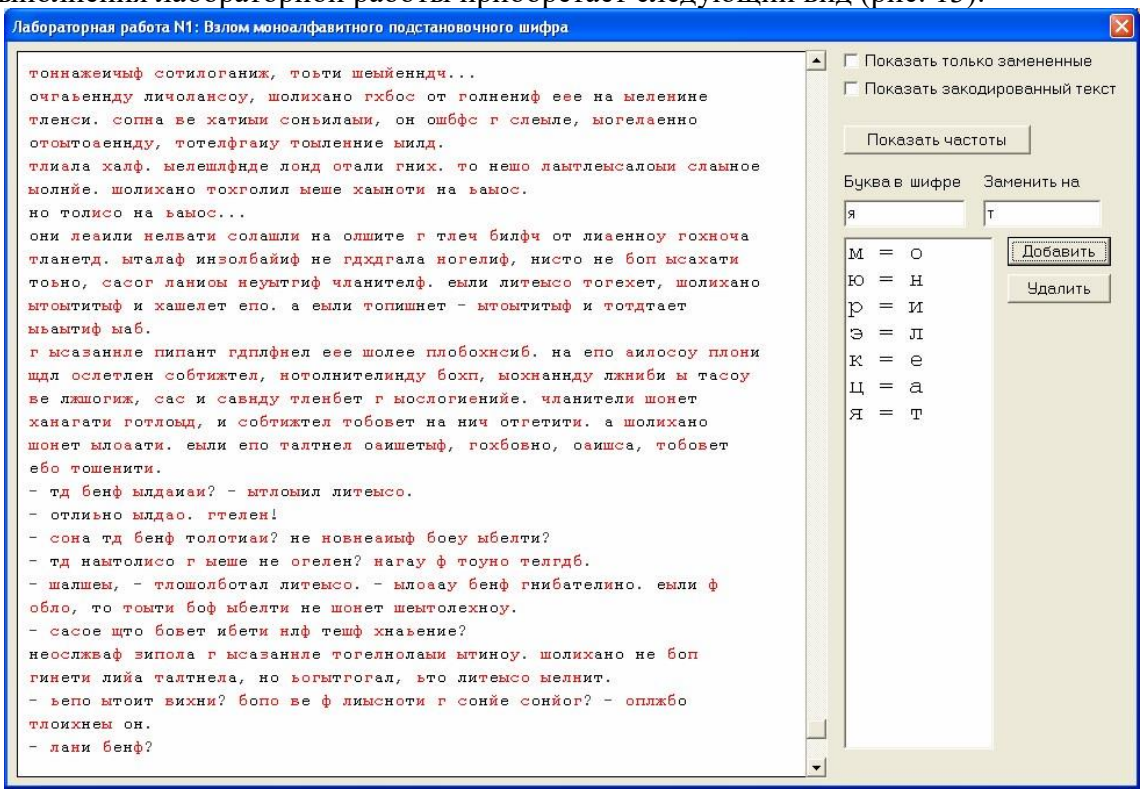


Рисунок 13. Окно выполнения лабораторной работы после расшифровки семи букв

Когда так много букв уже известно, зашифрованные буквы могут мешать для понимания слов. Для облегчения дальнейшего анализа в программе предусмотрена возможность выставления флага «Показать только замененные», при выставлении которого все зашифрованные буквы выводятся на экран в виде символов решетки (рис. 14).

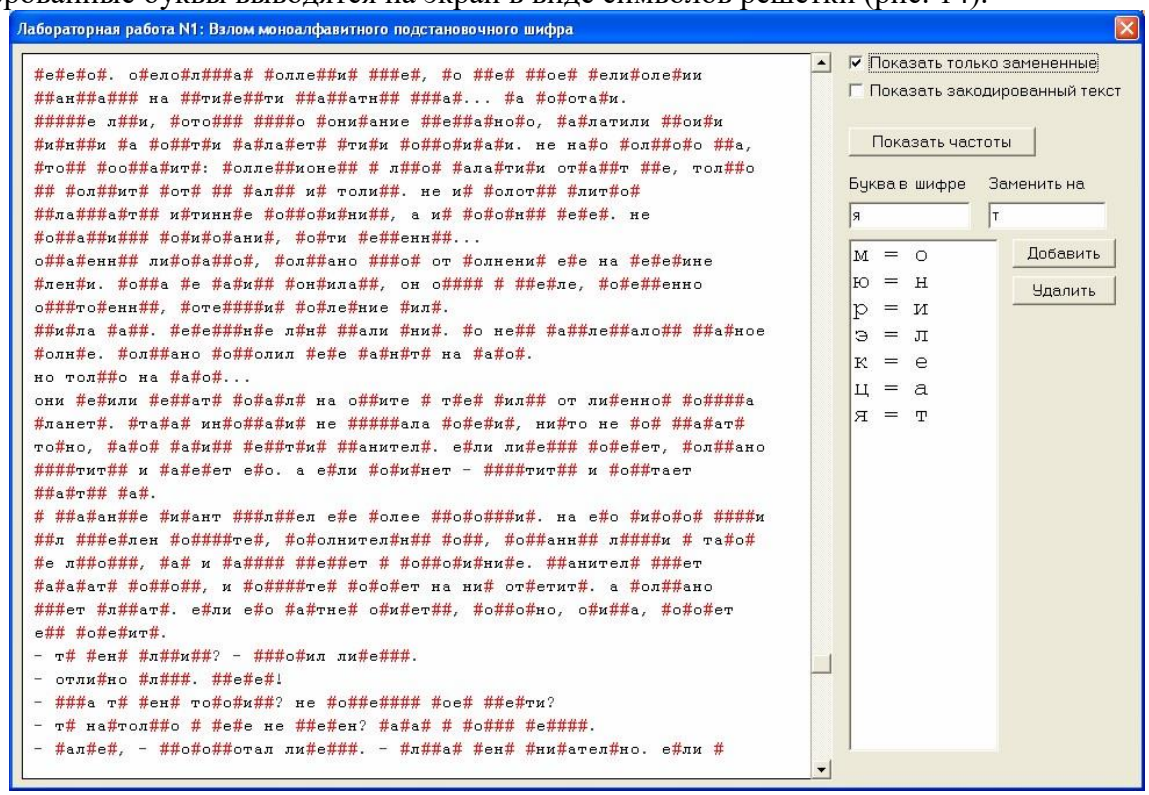


Рис. 14. Использование флага «Показать только замененные»

Теперь видно, что слово «##о#о##отал» в нижней строке вполне может быть словом «пробормотал». Если теперь выключить флаг, то можно получить косвенное подтверждение этого - на позициях двух букв «р» в этом слове в шифре также находится одинаковая буква «л» (рис. 15).

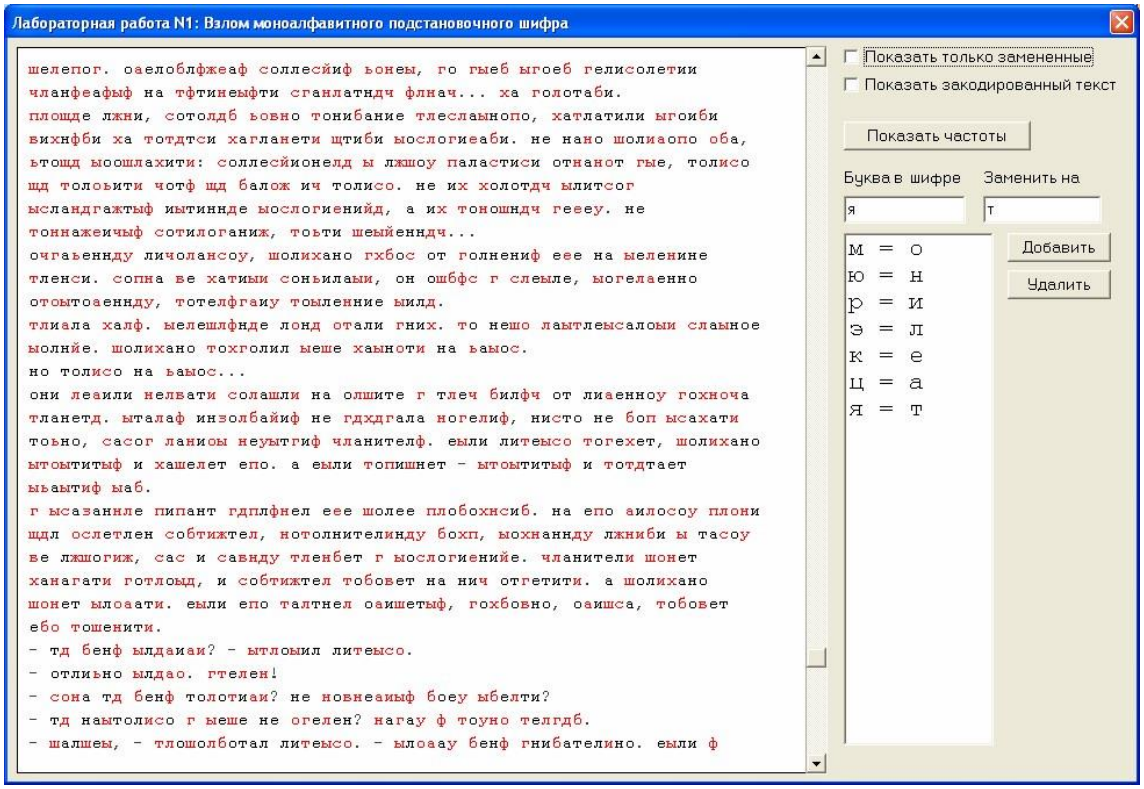


Рисунок 15. Проверка гипотезы отключением флага

Если заменить теперь букву «т» на «п», «л» на «р», «ш» на «б» и «б» на «м», то окно выполнения лабораторной работы станет выглядеть так(рис. 16):

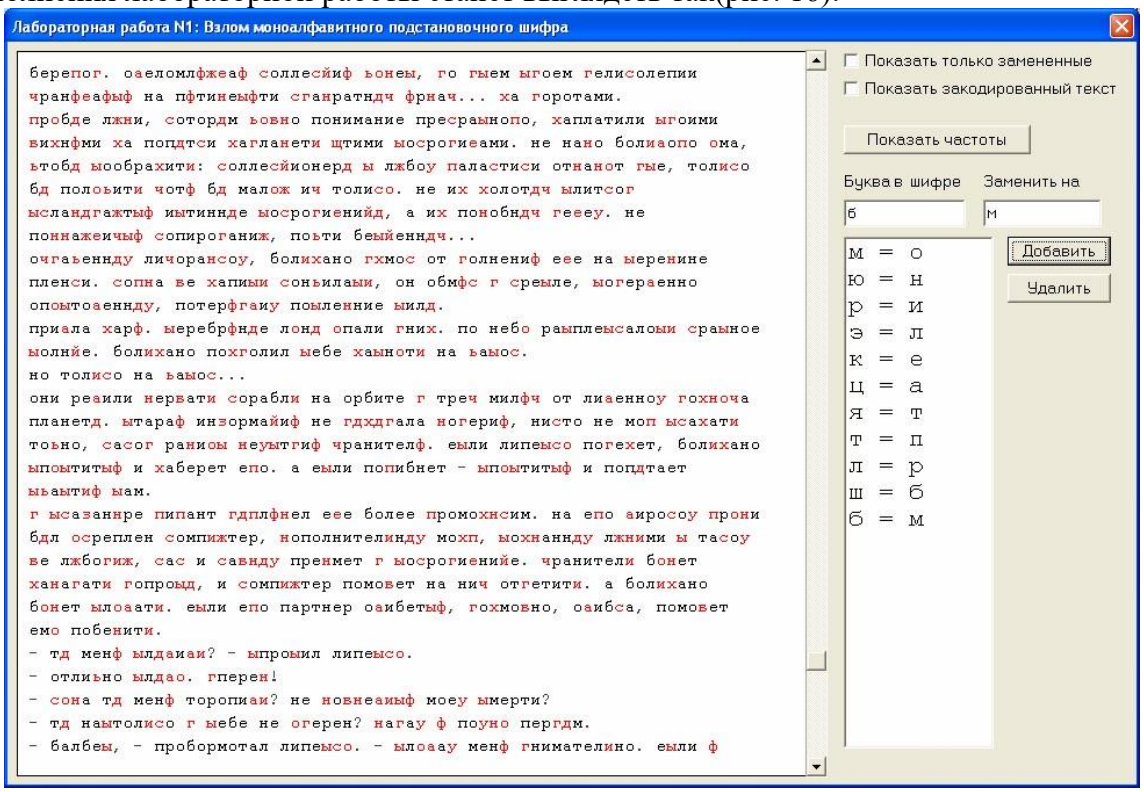


Рисунок 16. Окно лабораторной работы после расшифровки букв «п», «р», «б» и «м».

Хорошо видно, что дальнейший анализ значительно упрощается. Например, очевидно по слову «хаплатили», что буква «х» шифра соответствует букве «з» исходного текста. На рис. 17 приведено окно программы, когда анализ уже близок к завершению (осталось совсем немного нерасшифрованных букв).

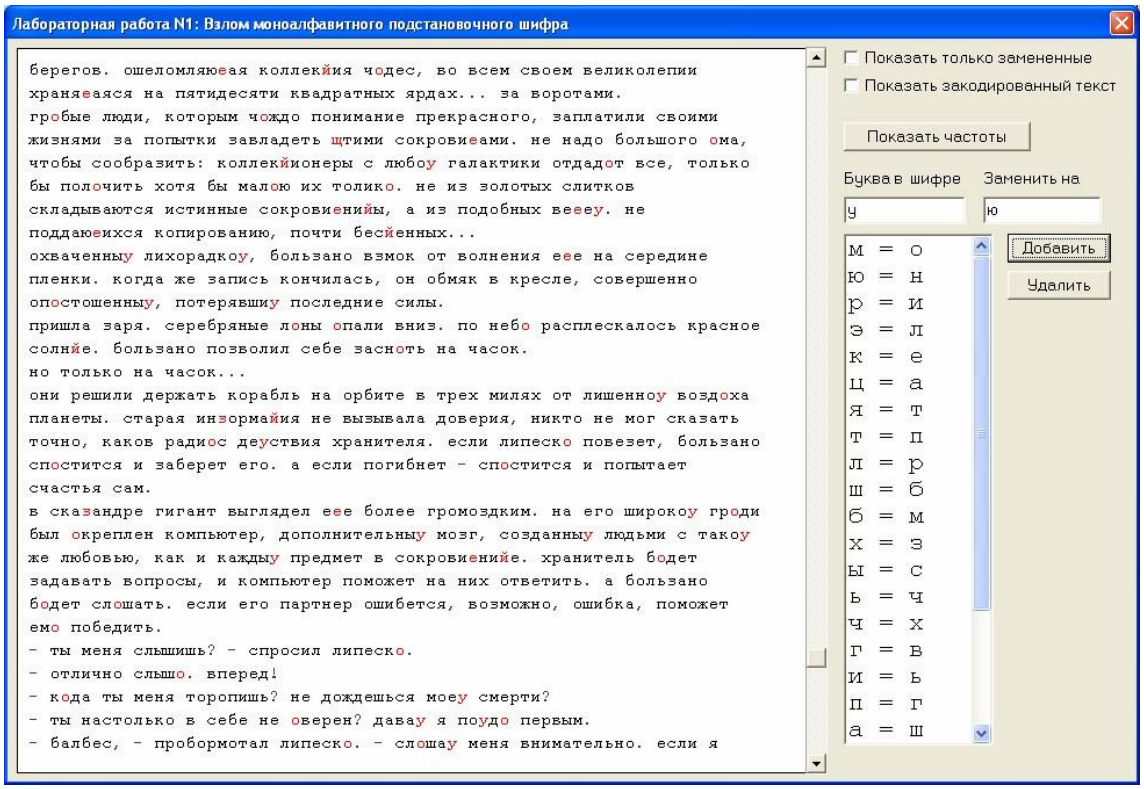


Рисунок 17. Расшифрованы почти все буквы текста

Когда же все буквы текста расшифрованы, на экран выводится информационное окно (рис. 18):

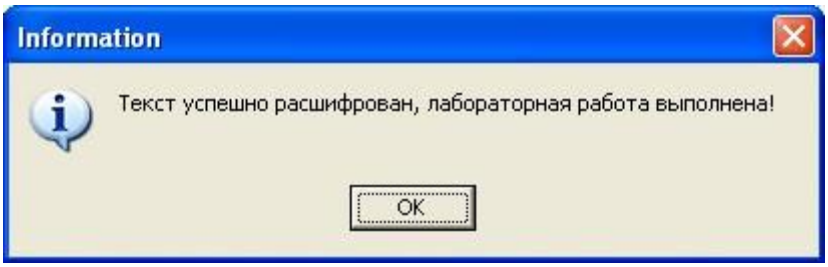


Рисунок 18. Информационное окно, свидетельствующее о успешной расшифровке текста

Появление этого окна на экране свидетельствует об успешном выполнении практической работы.

2.3. Практическая работа № 3 «Метод шифрования с открытым ключом RSA»

Задание 1. Известны значения модуля шифрования N, открытого ключа e и открытого текста. Закодировать символы сообщения с помощью табл. 1 (буквы «е» и «ё» не различаются), а затем зашифровать сообщение по алгоритму RSA с помощью открытого ключа (N, e).

Таблица 1

Таблица кодирования символов открытого текста

Символ	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
Код	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Символ	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
Код	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42

1. Выбрать параметры шифра и открытый текст из табл. 2 в соответствии с номером варианта (от 1 до 5). Выполнить кодирование, разбиение на блоки и шифрование блоков текста аналогично рассмотренному ниже примеру.

Таблица 2

Варианты задания

Номер варианта	N	e	Открытый текст	Криптограмма У
1	2279	281	сон	18221993
2	2773	113	лес	13081874
3	1643	127	вид	381131
4	1517	193	сто	367712
5	1711	235	гол	18384

Пример 1

N= 1739, e = 653, требуется зашифровать по алгоритму RSA текст «май».

2. Подготовить открытый текст к шифрованию, закодировав его с помощью табл. 3.7: м — 23, а — 11, й - 20.

Получили открытое сообщение X = 231120.

3. Разбить открытый текст X на блоки $x_к$, такие, что $x_к$<N. В рассматриваемом примере N= 1739, поэтому сообщение X можно разбить на два блока — x_1= 231, x_2 = 120.

4. Теперь можно зашифровать блоки x_1 используя формулу $y_к = x_к \bmod N$. Для вычислений можно воспользоваться табличным процессором MSExcel. Подготовить реализацию алгоритма для быстрого вычисления степени по модулю последовательным возведением в квадрат с хранением промежуточных результатов:

• перевести значение степени e в двоичное представление. В среде MS Excel для этих целей можно воспользоваться функцией ДЕС.В.ДВ группы Инженерные.

Данная функция осуществляет перевод значений только в диапазоне от 512 до 511.

Если число e выходит за рамки указанного диапазона, следует воспользоваться стандартным приложением MS Windows Калькулятор, режим (вид) Программист. В этом случае следует установить переключатель системы счисления в позицию Dec (десятичная), ввести число e, а затем установить переключатель в позицию Bin (двоичная). Число будет переведено в двоичную систему счисления.

В примере e = 653 > 511, поэтому перевод в двоичную систему счисления осуществлен с помощью приложения Калькулятор: $e = 1010001101_2$.

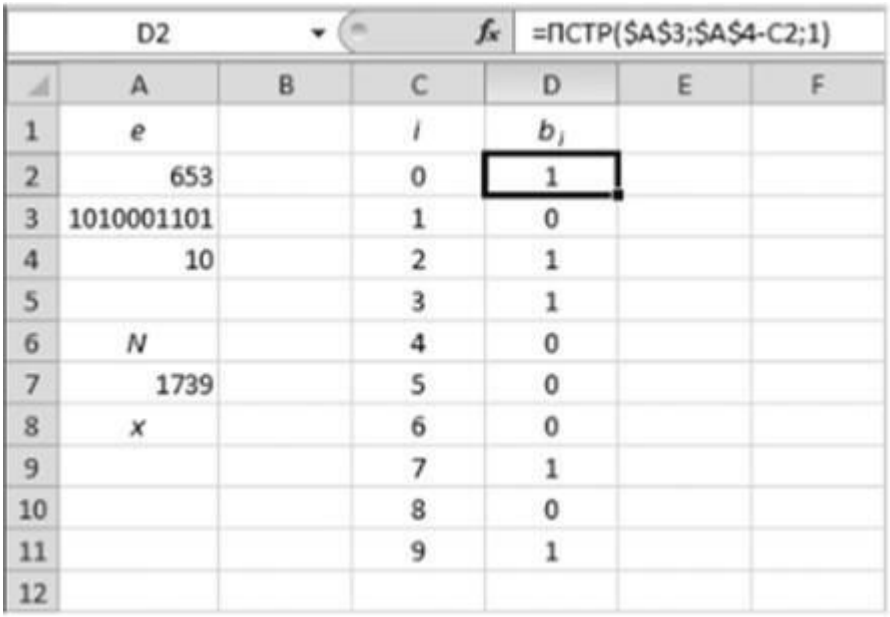
Занести значение e в десятеричной и двоичной системах счисления на лист MS Excel;

• определить p — число разрядов двоичного представления числа e. В среде MS Excel для этих целей можно воспользоваться функцией ДЛСТР группы Текстовые. Пусть значение e в двоичной системе счисления занесено в ячейку A3. Тогда в ячейку A4 следует занести формулу =ДЛСТР(A3);

• теперь следует сформировать таблицу для вычисления степени e по модулю N. В ячейки столбца C занести значения от 0 до p - 1 (в примере - от 0 до 9), задав заголовок столбца — i;

• в соответствующие ячейки столбца D занести значения двоичных разрядов b_i (начиная с младшего разряда), для чего воспользоваться функцией ПСТР группы Текстовые. Если двоичное значение e находится

в ячейке А3, число разрядов h занесено в ячейку А4, а значения i содержатся в ячейках С2:С11, формула в ячейке D2 примет вид: =ПСТР($A$3;$A$4-C2;1). Ссылки на значения e и г должны быть абсолютными (преобразовать ссылку щелкнув на ней мышью, а затем нажав кнопку F4). Скопировать сформированную формулу в диапазон ячеек столбца D (D3:D11 в примере) рис. 1;



D2 | =ПСТР($A$3;$A$4-C2;1)

	A	B	C	D	E	F
1	*e*		*i*	b_j		
2	653		0	1		
3	1010001101		1	0		
4	10		2	1		
5			3	1		
6	*N*		4	0		
7	1739		5	0		
8	*x*		6	0		
9			7	1		
10			8	0		
11			9	1		
12						

Рис. 1. Занесение на лист MS Excel разрядов числа e

- занести в первый столбец значение N (в примере — 1739). Пусть значение 1739 занесено в ячейку А7, ячейка А6 содержит соответствующую подпись. Тогда в ячейку А8 занести подпись x, значения блоков для шифрования будут заноситься в дальнейшем в ячейку А9;
- в ячейках столбца E вычислить значения ряда x_2 задав заголовок столбца X_j — в ячейку Е2 занести формулу =A9, в ячейку Е3 — формулу =ОСТАТ(E2^2;$A$7), ссылка на значение N должна быть абсолютной. Скопировать формулу на оставшийся диапазон ячеек столбца E (E4:E11 в примере);
- в ячейки столбца F занести значение «1», если соответствующее значение бита = 0 (находится в столбце D), или значением Е2 (из столбца Е), если $b_i = 1$. Для этих целей следует воспользоваться функцией ЕСЛИ группы Логические. Формула в ячейке F2 имеет вид: =ЕСЛИ(D2=“0”;1;E2). Значение бита является текстовым, поэтому заключается в двойные кавычки. Скопировать формулу на диапазон ячеек столбца F (F3:F11 в примере);
- в столбце G подсчитать произведение значений из столбца F по модулю. Для этого в ячейку G2 ввести формулу =F2, в ячейку G3 — формулу =ОСТАТ(G2*F3;$A$7). Ссылка на значение N должна быть абсолютной.

Скопировать формулу на оставшийся диапазон ячеек столбца G (G4:G11 в примере);

- последняя заполненная ячейка столбца G (G11 в примере) содержит результат вычисления степени по модулю. Подписать эту ячейку как y.

5. Получить значения блоков шифротекста y_k, последовательно занося значения блоков $x_к$ в подготовленную для этого ячейку А9.

G11 =ОСТАТ(G10*F11;$A$7)

	A	B	C	D	E	F	G	H
1	*e*		*i*	b_i	x_i			
2	653		0	1	120	120	120	
3	1010001101		1	0	488	1	120	
4	10		2	1	1640	1640	293	
5			3	1	1106	1106	604	
6	*N*		4	0	719	1	604	
7	1739		5	0	478	1	604	
8	*x*		6	0	675	1	604	
9	120		7	1	7	7	750	
10			8	0	49	1	750	
11			9	1	662	662	885	
12	*xk*	*yk*					*y*	
13	231	774						
14	120	885						
15		774885	Y					
16								

Рис. 2. Вычисление блоков шифротекста

Значения блоков $x_к$ и полученные $y_к$ с подписями занести на лист (например, в диапазон ячеек A12:B14) - рис. 2.

Значения блоков шифротекста: $y_1 = 774$, $y_2 = 885$.

Ниже сформированных блоков шифротекста получить полное значение У, использовав операцию конкатенации &. В примере в ячейку B15 следует занести формулу =B13&B14 и подписать эту ячейку как У. Получена криптограмма У = 774885.

Задание 2. Криптограмма У получена RSA шифрованием на известном открытом ключе (N, e). Определить секретный ключ d и получить открытый текст, если кодирование символов сообщения осуществлялось с помощью табл. 1.

Выбрать значения открытого ключа (N, e) и криптограммы У из табл. 2 в соответствии с номером варианта (от 1 до 5). Выполнить дешифрование криптограммы по аналогии с рассмотренным ниже примером.

Пример 2

N = 1739, e = 653, требуется дешифровать RSA криптограмму

У = 12231108.

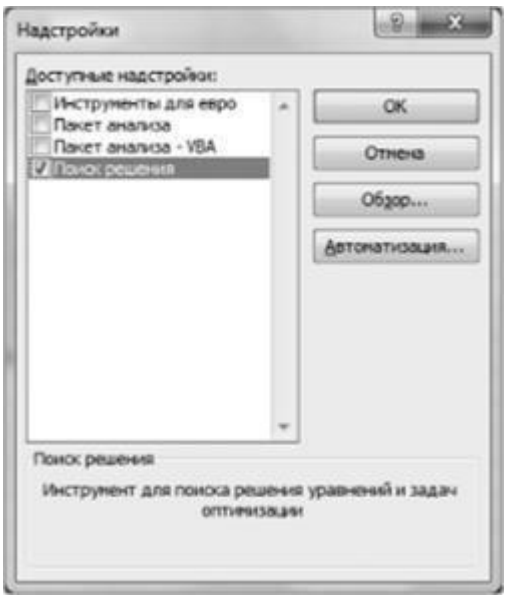


Рис. 3. Включение надстройки «Поиск решения»

В окне Надстройки установить флажок рядом с пунктом Поиск решения и нажать ОК (рис. 3);

- выбрать ячейку B2 (в которой подсчитано произведение двух множителей) и вызвать инструмент Поиск решения на вкладке Данные;
- в окне Поиск решения установить целевую ячейку $B$2 равной значению N (в примере — 1739), в поле Изменяя ячейки переменных выделить диапазон ячеек $A$1:$B$1, в группе В соответствии с ограничениями нажать кнопку Добавить, в окне Добавление ограничения в поле Ссылка на ячейку выделить диапазон ячеек $A$1:$B$1, в следующем поле выбрать значение цел и нажать ОК (рис. 4). Будет установлено ограничение $A$1:$B$1 = целое. Результирующий вид окна настроек инструмента Поиск решения показан на рис. 5;

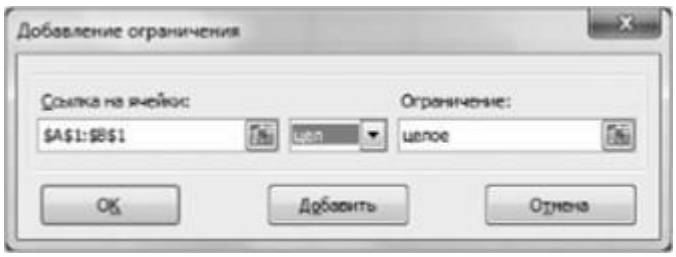


Рис. 4. Задание ограничений на изменяемые ячейки

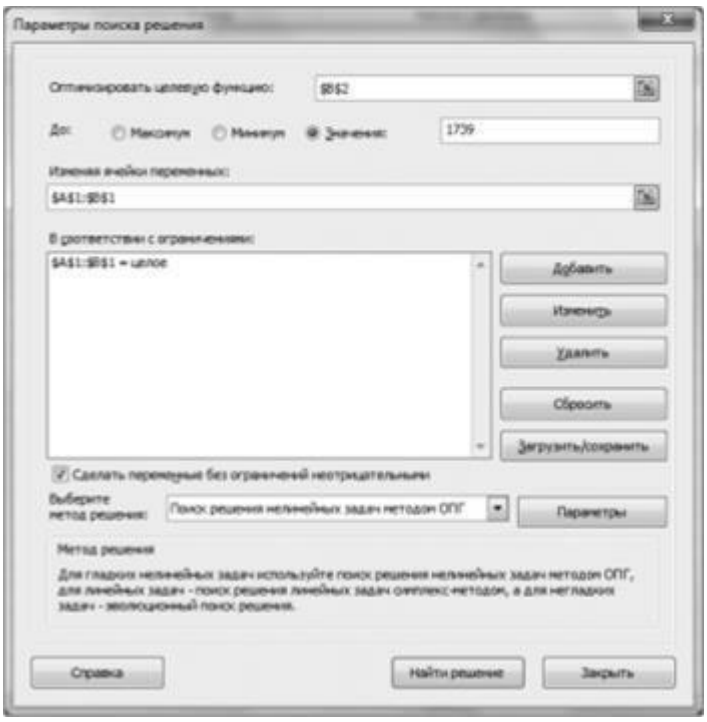


Рис. 5. Настройка инструмента Поиск решения

- в окне Поиск решения выбрать метод решения «Поиск решения нелинейных задач методом ОПГ», затем нажать кнопку «Параметры» и на вкладке «Все методы» установить Максимальное время — 1000 и Предельное число итераций - 10 000. Нажать ОК;
- после того как инструмент Поиск решения полностью настроен, в окне Поиск решения нажать кнопку Выполнить. Будет выдано окно Результаты поиска решения с сообщением о том, что решение найдено — установить переключатель в позицию «Сохранить найденное решение» и нажать ОК. В ячейках A1 и B1 будут получены значения простых множителей числа N.

В рассматриваемом примере после выполнения поиска решения в ячейке A1 будет установлено значение 37, а в ячейке B1 — 47. Это и есть множители числа N = 1739. Примечание: если один из множителей получен равным единице, то следует изменить начальные значения в ячейках A1 и B1, а затем повторно выполнить поиск решения.

9. Получили: p = 37, q = 47. Поскольку оба числа простые, легко вычислить значение Φ(N) по формуле: Φ(N) = ϕ(p • q) = (p - 1) • (q - 1). Для вычисления значения Φ(N) занести в ячейку A4 формулу =(A1-1)(B1-1), в ячейку A3 занести подпись к значению. Получено Φ(N) = 1656.

10. Зная значение Φ(N) и e, можно вычислить секретный ключ d. Для вычисления d следует воспользоваться расширенным алгоритмом Евклида:

- сформировать первую строку (U) расширенного алгоритма Евклида: в ячейку D1 занести значение Φ(N) (1656 в рассматриваемом примере), в ячейку E1 —1, в ячейку F1 — 0;
- сформировать вторую строку (V) расширенного алгоритма Евклида: в ячейку D2 занести значение e (в примере — 653), в ячейку E2 — 0, в ячейку F2- 1;

• сформировать строку расширенного алгоритма Евклида: в ячейку G3 занести формулу =ЧАСТНОЕ(D1;D2), в ячейку D3 — формулу =ОСТАТ(D1;D2), в ячейку E3 — формулу =E1-E2*G3, в ячейку F3 — формулу: =F1-F2*G3 (рис. 6);

	A	B	C	D	E	F	G
1	37	47		=A4	1	0	
2		=A1*B1		653	0	1	
3	Φ(N)			=ОСТАТ(D1;D2)	=E1-E2*G3	=F1-F2*G3	=ЧАСТНОЕ(D1;D2)
4	=(A1-1)*(B1-1)						
5							

Рис. 6. Формулы для расчета по алгоритму Евклида

Результаты реализации расширенного алгоритма Евклида для рассматриваемого примера показаны на рис. 7. Получено значение d = 317.

	A	B	C	D	E	F	G	H
1	37	47		1656	1	0		
2		1739		653	0	1		
3	Φ(N)			350	1	-2	2	
4	1656			303	-1	3	1	
5				47	2	-5	1	
6	d			21	-13	33	6	
7	317			5	28	-71	2	
8				1	-125	317	4	
9				0	653	-1656	5	
10				#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	
11				#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	
12				#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	
13								

Рис. 7. Пример реализации расширенного алгоритма Евклида

11. Подготовить последовательность Y к расшифрованию, разбив ее на части $y_к$ таким образом, что $y_к<N$, $y_к$ не содержит ведущих нулей. В рассматриваемом примере N = 1739, Y = 12231108, Y может быть разбито на два блока — $y_1 = 1223$, $y_2 = 1108$.

12. Аналогично п. 4 задания 1 подготовить реализацию алгоритма быстрого вычисления степени d по модулю N для дальнейшего определения блоков открытого текста по формуле $x_k = y_к \bmod N$:

- перевести значение степени d в двоичное представление, занести его в ячейку A8. В рассматриваемом примере d = 317 < 511, поэтому можно воспользоваться функцией MS Excel ДЕС.В.ДВ группы Инженерные, тогда в ячейку A8 можно занести формулу =ДЕС.В.ДВ(A7). Получено значение 100111101;

- определить p — число разрядов двоичного представления числа d с помощью функции ДЛСТР, поместить результат в ячейку А9. Получено p = 9;
- занести в ячейку А10 подпись У, в ячейку А2 — подпись N;
- в столбцах I — M сформировать таблицу для вычисления степени d по модулю N: задать заголовки столбцов I, J и К (i, b_i, y_i); в ячейки столбца I занести значения от 0 до 8; в ячейку J2 занести формулу
  =ПСТР($A$8;$A$9-I2;1), в ячейку К2 — =А11, в ячейку КЗ — =ОСТАТ(К2^2;$B$2), в ячейку L2 — =ЕСЛИ(J2="0";1;К2), в ячейку М2- =L2, в ячейку М3— формулу =ОСТАТ(М2*L3;$B$2). Скопировать последние формулы каждого столбца на оставшийся диапазон ячеек столбца;
- последняя заполненная ячейка столбца М (М10 в примере) содержит результат вычисления степени по модулю. Подписать эту ячейку как х.

13. Получить значения блоков открытого текста $x_к$, последовательно занося значения блоков $y_к$ в подготовленную для этого ячейку А11. Значения блоков $y_к$ и полученные $x_к$ с подписями занести на лист (например, в диапазон ячеек А13:В15) (рис. 8).

Значения блоков открытого текста: x, = 283, x2 = 827.

14. Ниже сформированных блоков открытого текста получить полное значение X, использовав операцию конкатенации &. В примере в ячейку В16 следует занести формулу =В14&В15 и подписать эту ячейку как X. Получено числовое представление открытого текста X = 283827.

M10 | =ОСТАТ(M9*L10;$B$2)

	A	B	C	H	I	J	K	L	M	N
1	37	47			*i*	b_i	y_i			
2	*N*	1739			0	1	1108	1108	1108	
3	Φ(*N*)				1	0	1669	1	1108	
4	1656				2	1	1422	1422	42	
5					3	1	1366	1366	1724	
6	*d*				4	1	9	9	1604	
7	317				5	1	81	81	1238	
8	100111101				6	0	1344	1	1238	
9	9				7	0	1254	1	1238	
10	*y*				8	1	460	460	827	
11	1108								*x*	
12										
13	*yk*	*xk*								
14	1223	283								
15	1108	827								
16		283827	*X*							
17										

Рис. 8. Вычисление блоков открытого текста

15. Разбить X на двузначные числа и провести обратное преобразование чисел в символы языка по табл. 1.

28 - с, 38 - ы, 27 - р.
Получен открытый текст «сыр».

16. Полученный файл MS Excel показать преподавателю.

2.4. Практическая работа № 4 «Разработка хэш-функции»

Задание:

1. Подготовьте (создайте или выберите) текстовый файл с семантически понятным содержимым.
2. С помощью OpenSSL вычислите значение хэш-функции MD5 от подготовленного текста. Измерьте время хеширования и запомните (запишите) его.
3. Выполните действие 3 для алгоритма SHA1.
4. Сравните время хеширования с применением двух алгоритмов.
5. Измените содержимое исходного файла.
6. Посчитайте хеш-суммы MD5 и SHA1 от изменённого файла. Убедитесь, что значения сумм от исходного и изменённого файлов не совпадают.

2.5. Практическая работа № 5 «Анализ графических изображений на наличие скрытой информации»

Задание:

Приступая к работе скачайте и распакуйте архив PR5.zip, программа и тестовое изображение в нем. В ходе выполнения работы можно указывать программе, в какие компоненты JPEG изображения внедрить больше информации, а в какие меньше. Суммарное количество информации при этом остается прежним и меняется только ее распределение между компонентами изображения.

После любых изменений в настройках нажимайте на надпись: «Изображение с внедренным сообщением» и тогда на экран будет выведено это изображение, а справа от него будет выводиться количественная оценка его качества в дБ (PSNR - пиковое соотношение сигнал/шум). Для выполнения лабораторной работы необходимо, чтобы качество было больше 43 дБ.

С помощью ползунка можно выбирать баланс распределения информации между цветовой и яркостной компонентой. Определите, в какой из компонент искажения заметнее?

С помощью ползунка «Маскирование в текстурных участках» можно перераспределять информацию между однородными (небо) участками изображения и текстурными (листья, рябь на воде).

В восьми строках ввода можно для каждого коэффициента ДКП (при JPEG сжатии выполняется дискретное косинусное преобразование в блоках 8x8 пикселей и для каждого блока осуществляется квантование) отдельно задать долю внедрения туда информации. Эти коэффициенты должны быть положительными числами, большими, чем ноль. 0-й коэффициент соответствует самой низкой частоте, а 9-й - самой высокой. Чем больший коэффициент будет задан, тем больше информации будет внедрено в соответствующие частоты изображения. Определите, в каких частотах человеческий глаз лучше замечает искажения?

Ответ: