© Минзов А.С.

**Лабораторная работа № 3**

**Основы криптографии**

*Лабораторная работа выполняется с использованием электронных таблиц или в программной среде по выбору студента.*

**Список заданий:**

1. Изучить и применить метод моноалфавитной замены для шифрования/дешифрования текста.
2. Изучить и применить метод перестановки для шифрования/дешифрования текста.
3. (*Опционально*). Изучить и применить метод дробления для шифрования/дешифрования текста.

**Дополнительная информация и рекомендации по выполнению**

КРИПТОГРАФИЯ **—** наука и искусство передачи сообщений в таком виде, чтобы их нельзя было прочитать без специального секретного ключа. Слово «криптография» происходит от древнегреческих слов kryptos "секрет" и graphos "писание". Исходное сообщение называется в криптографии открытым текстом, или клером. Засекреченное (зашифрованное) сообщение называется шифротекстом, или шифрограммой, или криптограммой. Процедура шифрования обычно включает в себя использование определенного алгоритма и ключа. Алгоритм – это определенный способ засекречивания сообщения, например компьютерная программа или список инструкций. Ключ же конкретизирует процедуру засекречивания.

**Задание 1.**

## Справочная информация

### Шифрование методом моноалфавитной замены

Один из способов шифрования – ПРОСТАЯ ЗАМЕНА, при которой каждая буква открытого текста заменяется на какую-то букву алфавита (возможно, на ту же самую). Для этого отправитель сообщения должен знать, на какую букву в шифротексте следует заменить каждую букву открытого текста. Часто это делается путем сведения нужных соответствий букв в виде двух алфавитов, например, так, как показано ниже в таблице, где первая строка соответствует открытому алфавиту, а вторая — закрытому (шифровальному):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | L | U | E | S | T | O | C | K | I | N | G | A | D | F | H | J | M | P | Q | R | V | W | X | Y | Z |

Шифрограмма получается путем замены каждой буквы открытого текста на записанную непосредственно под ней букву шифровального алфавита.

Пусть требуется зашифровать следующее сообщение (открытый текст):

DEAR DAD

SEND MORE MONEY AS SOON AS POSSIBLE TOM

(Дорогой папа. Как можно скорее пришли еще денег. Том.)

Используя приведенную таблицу, получаем D->E, E->S, A->B и т.д. Таким образом будет получена шифрограмма:

ESBM EBE

HGSBPS PSDE AFMS AFDSY BP PFFD BP HFPPKLGS QFA

Две алфавитные последовательности, используемые в процессе шифрования, называются, соответственно, открытым и шифровальным компонентом системы. Чтобы получатель шифрограммы мог восстановить открытый текст и прочитать сообщение, ему необходимо иметь копию вышеприведенной таблицы. Дешифровщик повторяет в обратном порядке все действия шифровальщика, раскрывая тем самым содержание сообщения.

В вышеприведенном примере использовался алгоритм побуквенной замены. Этот метод называется ПРОСТОЙ, или МОНОАЛФАВИТНОЙ заменой. Ключ к данному шифру состоит из таблицы, содержащей открытый и шифровальный алфавиты, в которой указывается, на какую букву в шифротексте следует заменить букву открытого текста. В такой криптографической системе предполагается, что алгоритм шифрования общеизвестен, тогда как ключ доступен только отправителю и получателю соответствующих сообщений.

В открытом алфавите буквы расположены в их обычной последовательности; такой алфавит называется прямой стандартной последовательностью. Шифровальный же алфавит в нашем примере состоит из 26 букв латинского алфавита, определенным образом переставленных с использованием ключевого слова BLUESTOCKING (букв. «синий чулок»). После ключевого слова (ключевой фразы) ключ далее записывается с опущением всех тех букв, что уже появились в этом слове (или в этой фразе), а затем вписываются остающиеся буквы алфавита в обычном порядке, опять же с опущением всех ранее появившихся букв.

Так, если в качестве ключевой мы используем фразу UNITED STATES OF AMERICA, то начало шифровального алфавита будет состоять из неповторяющихся букв в этой фразе:

U N I T E D S A O F M R C

Осталось дополнить ее оставшимися буквами открытого алфавита в обычном порядке, опуская при этом ранее включенные буквы. Таким образом шифровальный алфавит будет выглядеть следующим образом:

U N I T E D S A O F M R C B G H J K L P Q V W X Y Z

С помощью ключевого слова (фразы) при шифровании можно перемешать любую алфавитную последовательность. Использование ключевых слов облегчает восстановление открытого и шифровального компонента системы, поскольку при этом необходимо запомнить только соответствующее ключевое слово (фразу). Нет необходимости записывать (или разгадывать) какие бы то ни было таблицы: если помнить ключевое слово, то алфавитную последовательность всегда можно восстановить по памяти.

В вышеприведенной шифрограмме между словами сохранены пробелы, однако шифровку можно сделать более защищенной (или, как говорят криптографы, устойчивой, или стойкой ко взлому; шифр считается тем более стойким, чем дольше он не поддается вскрытию) путем удаления межсловных пробелов из окончательного шифротекста. Согласно установившейся практике, шифротекст принято делить на группы из пяти букв каждая (когда-то телеграфные компании при взимании платы каждую группу из пяти букв считали, как одно слово открытого текста.) Если убрать пробелы между словами в нашей шифрограмме и разделить ее на группы по пять символов, то она приобретет следующий вид:

ESBME BEMGS BPSPS DEAFM SAFDS YBPPF FDBPH FPPKL GSQFA

Таким образом, алгоритм шифрования состоит из следующих шагов:

*Шаг 1*. Привести все буквы в ключевой фразе к одному регистру (все прописные или все строчные). Из ключевой фразы исключить межсловные пробелы, знаки препинания и незначащие символы, затем слева направо убрать повторяющиеся символы.

*Шаг 2*. К полученной строке добавить неповторяющиеся буквы алфавита в порядке их следования и создать шифровальный алфавит. Подготовить таблицу для замены соответствующих символов открытого алфавита на символы закрытого алфавита, например в первом столбце разместить открытый алфавит, а во втором — шифровальный. Тогда буквы одной строки образуют пару для замены символа открытого текста на символ шифротекста и наоборот.

*Шаг 3*. Подготовить текст для шифрования: привести все буквы в исходном тексте к одному регистру (тому же, что был использован на шаге 1); исключить межсловные пробелы, знаки препинания и незначащие символы. Заменить далее побуквенно символы текста для шифрования на символы полученного алфавита в соответствии с подготовленной таблицей замены.

*Шаг 4*. Разделить полученную последовательность на группы по 5 символов.

## Выполнение задания

1. Выбрать в Приложении 1 исходный текст для шифрования согласно номеру вашего варианта.
2. Выбрать ключевую фразу в Приложении 2, которая определяется номером варианта.
3. Разработать программу шифрования текста (с помощью электронных таблиц или в программной среде), в которой:
   1. Предусмотреть ввод ключевой фразы, перевод всех букв этой фразы в один регистр и удаление из нее незначащих символов, знаков препинания и пробелов.
   2. Обеспечить преобразование ключевой фразы в новый алфавит и подготовку таблицы замены (шаг 1 и шаг 2 описанного алгоритма шифрования).
   3. Обеспечить ввод текста для шифрования, перевод всех букв в один регистр и удаление из текста незначащих символов знаков препинания и пробелов.
   4. Зашифровать текст (шаг 3 и шаг 4 алгоритма).
4. Провести расшифрование шифрованного текста.

При выполнении задания используются любые технологии по выбору студента: электронные таблицы, *VBA* *for application* (*Excel*), *Java*, *JavaScript*, *PHP*, *C# C++*, *Phyton* и т. п.

*В отчете необходимо описать с помощью каких функций Excel выполнена реализация алгоритма, или представить исходный текст программы с обязательными комментариями, поясняющими назначение и алгоритм работы методов.*

**Задание 2.**

## Справочная информация

### Шифрование методом перестановки

Другим важнейшим шифровальным алгоритмом является ПЕРЕСТАНОВКА. В шифре перестановки все буквы открытого текста остаются без изменений, но переставляются согласно заранее оговоренному правилу. Здесь также может использоваться ключ, управляющий процедурой шифрования. Так, используя в качестве ключа слово PANAMA, мы могли бы зашифровать вышеупомянутый открытый текст следующим образом:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ключ** | **P** | **A** | **N** | **A** | **M** | **A** |
| **Числовая последовательность** | **6** | **1** | **5** | **2** | **4** | **3** |
| **Блок перестановки** | D | E | A | R | D | A |
|  | D | P | L | E | A | S |
|  | E | S | E | N | D | M |
|  | O | N | E | Y | A | S |
|  | S | O | O | N | A | S |
|  | P | O | S | S | I | B |
|  | L | E | T | O | M |  |
|  | DDEOSPL | EPSNOOE | ALEEOST | RENYNSO | DADAAIM | ASMSSB |
| Шифрограмма | EPSNO OEREN YNSOA SMSSB DADAA IMALE EOSTD DEOSP L | | | | | |

В этом примере ключевое слово использовано для получения шифровальной числовой последовательности путем нумерации букв ключевого слова (относительно друг друга) в порядке их следования слева направо в стандартном алфавите. Например, буква «**A**» в первом слоге получила номер **1**, она же во втором слоге получила номер **2** и т. д. Далее под числовой последовательностью в строках, равных по длине ключевому слову, записан открытый текст. В процессе шифрования текст выписывается уже по отдельным столбцам в порядке, определяемом данной числовой последовательностью. То есть первыми в шифрограмме будут символы из столбца, соответствующего цифре **1** числовой последовательности (EPSNOOE), затем цифре **2** (RENYNSO) и т. д. Последний шаг — разделение полученного шифротекста на группы по 5 букв.

Этот метод перестановки называется перестановкой столбцов, но можно избрать и другие «маршруты» перестановки, например выписывать шифротекст следуя по диагонали (слева направо или справа налево, или же чередуя левое и правое направления) или по спирали и т. п. Кроме того, буквы шифротекста могут записываться, следуя контурам различных геометрических фигур, или любыми другими способами. Один из них состоит в двойном шифровании путем повторной перестановки столбцов. При этом и в первом, и во втором блоках перестановки может быть использовано одно и то же ключевое слово, хотя лучше использовать разные ключевые слова. Такой шифр, называющийся двойной перестановкой, получил широкое распространение в 20 веке.

## Выполнение задания

Используя в качестве ключевого слова вашу фамилию, имя или другое слово (не менее 5 символов:

1) Зашифровать текст ключевой фразы вашего задания с помощью описанного метода перестановки столбцов;

2) Расшифровать заданный текст перестановкой столбцов с помощью выбранного ключевого слова. Текст, полученный в 1), является исходным при выполнении этого пункта.

При выполнении задания используются любые технологии по выбору студента: электронные таблицы, *VBA* *for application* (*Excel*), *Java*, *JavaScript*, *PHP*, *C# C++*, *Phyton* и т. п.

*В отчете необходимо описать с помощью каких функций Excel выполнена реализация алгоритма, или представить исходный текст программы с обязательными комментариями, поясняющими назначение и алгоритм работы методов.*

**Задание 3 (*опционально*).**

## Справочная информация

Третьим основным алгоритмом шифрования является ДРОБЛЕНИЕ. При этом каждой букве открытого текста сопоставляется более одного символа шифротекста, после чего символы перемешиваются (переставляются) в определенном порядке.

### Механизм шифрования на основе метода дробления

Ниже приведена таблица, демонстрирующая процедуру дробления с использованием знаменитого шифра Bifid, авторство которого приписывается французскому криптографу Феликсу Мари Деластеллю. Алгоритм описан на примере шифровального алфавита на основе ключевой фразы. Сначала составляется шифровальная таблица размером 5x5 (т.н. полибианский квадрат), куда построчно вписан шифровальный алфавит с ключевой фразой UNITED STATES OF AMERICA; причем ради того, чтобы общее число букв алфавита не превышало 25, буква J опускается (поскольку эта буква, с одной стороны, малоупотребительна в английских текстах, а с другой – вполне может быть заменена буквой I, без какого-либо урона для смысла). В данной таблице букве A, например, соответствуют координаты (2,3), букве B – (3,4) и т.д. Далее, в процессе шифрования под каждой буквой открытого текста в столбик записываются ее табличные координаты – номер строки и, ниже, номер столбца, а затем получившаяся цифровая последовательность переводится с помощью той же таблицы обратно в буквенную форму, но на этот раз она читается уже в строчку, т.е. (2,1) – буква D, (2,3) – буква A, (2,2) – буква S и т.д. При таком шифровании координата строки и координата столбца каждой буквы оказываются разъединенными, что характерно именно для раздробляющего шифра.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ключевая фраза | UNITED STATES OF AMERICA | | | | | | | |
| **Полибианский квадрат** |  |  | 1 | 2 | 3 | 4 | 5 | Шифровальный алфавит  (см. Задание 1),  вписанный построчно в квадрат |
|  | 1 | U | N | I | T | E |
|  | 2 | D | S | A | O | F |
|  | 3 | M | R | C | B | G |
|  | 4 | H | K | L | P | Q |
|  | 5 | V | W | X | Y | Z |
| **Открытый текст** | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | D | E | A | R | D | A | D | P | L | E | A | S | E | S | E | N | D | M | O | R | E | M | O | N | E | Y | | | | | | | | |
| **Координата строки** | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 2 | 1 | 2 | 3 | 2 | 2 | 2 | 4 | 4 | 1 | 2 | 2 | 1 | 2 | 1 | 1 | 2 | 3 | 2 | 3 | 1 | 3 | 2 | 1 | 1 | 5 | | | | | | | | |
| **Координата столбца** | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 1 | 5 | 3 | 2 | 1 | 3 | 1 | 4 | 3 | 5 | 3 | 2 | 5 | 2 | 5 | 2 | 1 | 1 | 4 | 2 | 5 | 1 | 4 | 2 | 5 | 4 | | | | | | | | |
| **Шифротекст** | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | D | A | S | O | H | S | N | U | A | A | I | D | E | E | R | I | T | G | R | W | W | U | K | V | K | Y | | | | | | | | |

Замена, перестановка и дробление представляют собой основные криптографические алгоритмы. Эти три базовых преобразования, зачастую в сочетании друг с другом, используются в большинстве систем шифрования для создания очень сложных шифровальных алгоритмов, особенно когда шифрование производится компьютером.

## Выполнение задания

1) Текст для шифрования и ключевая фраза находятся в Приложениях 1 и 2 соответственно и выбираются согласно номеру варианта.

2) Подготовить шифровальный алфавит по алгоритму, указанному в задании 1 и создать полибианский квадрат. Необходимо учесть, что для шифрования текстов на русском языке используется полибианский квадрат размером 6х6. Из полного алфавита обычно исключаются буквы Ё, Ъ; пять ячеек в квадрате останутся пустыми.

3) Используя созданный полибианский квадрат зашифровать первую строку текста для шифрования.

4) Используя созданный полибианский квадрат расшифровать текст, определенный в пункте 3).

*В отчете необходимо описать с помощью каких функций Excel выполнена реализация алгоритма, или представить исходный текст программы с обязательными комментариями, поясняющими назначение и алгоритм работы методов.*

Приложение 1.

## Исходный текст для кодирования

**1.** Пока приезжий господин осматривал свою комнату, внесены были его пожитки: прежде всего чемодан из белой кожи, несколько поистасканный, показывавший, что был не в первый раз в дороге. Чемодан внесли кучер Селифан, низенький человек в тулупчике, и лакей Петрушка, малый лет тридцати, в просторном подержанном сюртуке, как видно с барского плеча.

**2.** Вслед за чемоданом внесен был небольшой ларчик красного дерева с штучными выкладками из карельской березы, сапожные колодки и завернутая в синюю бумагу жареная курица. Когда все это было внесено, кучер Селифан отправился на конюшню возиться около лошадей, а лакей Петрушка стал устраиваться в маленькой передней, очень темной конурке.

**3.** В этой конурке он приладил к стене узенькую трехногую кровать, накрыв ее небольшим подобием тюфяка, убитым и плоским, как блин, и, может быть, так же замаслившимся, как блин, который удалось ему вытребовать у хозяина гостиницы. Покамест слуги управлялись и возились, господин отправился в общую залу. Какие бывают эти общие залы — всякий проезжающий знает очень хорошо.

**4.** Те же стены, выкрашенные масляной краской, потемневшие вверху от трубочного дыма и залосненные снизу спинами разных проезжающих., а еще более туземными купеческими, ибо купцы по торговым дням приходили сюда сам-шест и сам-сём испивать свою известную пару чаю; тот же закопченный потолок; та же копченая люстра со множеством висящих стеклышек.

**5.** Подобная игра природы, впрочем, случается на разных исторических картинах, неизвестно в какое время, откуда и кем привезенных к нам в Россию, иной раз даже нашими вельможами, любителями искусств, накупившими их в Италии по совету везших их курьеров. Господин скинул с себя картуз и размотал с шеи шерстяную, радужных цветов косынку.

**6.** Размотавши косынку, господин велел подать себе обед. Покамест ему подавались разные обычные в трактирах блюда, как-то: щи с слоеным пирожком, нарочно сберегаемым для проезжающих в течение нескольких неделей, мозги с горошком, сосиски с капустой, пулярка жареная, огурец соленый и вечный слоеный сладкий пирожок.

**7.** Как в просвещенной Европе, так и в просвещенной России есть теперь весьма много почтенных людей, которые без того не могут покушать в трактире, чтоб не поговорить с слугою, а иногда даже забавно пошутить над ним. Впрочем, приезжий делал не всё пустые вопросы; он с чрезвычайною точностию расспросил, кто в городе губернатор, кто председатель палаты, кто прокурор.

**8.** В приемах своих господин имел что-то солидное и высмаркивался чрезвычайно громко. Неизвестно, как он это делал, но только нос его звучал, как труба. Это, по-видимому, совершенно невинное достоинство приобрело, однако ж, ему много уважения со стороны трактирного слуги, так что он всякий раз, когда слышал этот звук, встряхивал волосами, спрашивал: не нужно ли чего?

**9.** После обеда господин выкушал чашку кофею и сел на диван, подложивши себе за спину подушку, которую в русских трактирах вместо эластической шерсти набивают чем-то чрезвычайно похожим на кирпич и булыжник. Тут начал он зевать и приказал отвести себя в свой нумер, где, прилегши, заснул два часа. Отдохнувши, он написал на лоскутке бумажки, по просьбе трактирного слуги, чин, имя и фамилию.

**10.** Когда половой все еще разбирал по складам записку, сам Павел Иванович Чичиков отправился посмотреть город, которым был, как казалось, удовлетворен, ибо нашел, что город никак не уступал другим губернским городам: сильно била в глаза желтая краска на каменных домах и скромно темнела серая на деревянных. Домы были в один, два и полтора этажа, с вечным мезонином.

**11.** Местами эти дома казались затерянными среди широкой, как поле, улицы и нескончаемых деревянных заборов; местами сбивались в кучу, и здесь было заметно более движения народа и живости. Попадались почти смытые дождем вывески с кренделями и сапогами, кое-где с нарисованными синими брюками и подписью какого-то Аршавского портного

**12.** Где магазин с картузами, фуражками и надписью: «Иностранец Василий Федоров»; где нарисован был бильярд с двумя игроками во фраках, в какие одеваются у нас на театрах гости, входящие в последнем акте на сцену. Игроки были изображены с прицелившимися киями, несколько вывороченными назад руками и косыми ногами, только что сделавшими на воздухе антраша.

**13.** Под всем этим было написано: «И вот заведение». Кое-где просто на улице стояли столы с орехами, мылом и пряниками, похожими на мыло; где харчевня с нарисованною толстою рыбою и воткнутою в нее вилкою. Чаще же всего заметно было потемневших двуглавых государственных орлов, которые теперь уже заменены лаконическою надписью: «Питейный дом».

**14.** Мостовая везде была плоховата. Он заглянул и в городской сад, который состоял из тоненьких дерев, дурно принявшихся, с подпорками внизу, в виде треугольников, очень красиво выкрашенных зеленою масляною краскою. Впрочем, хотя эти деревца были не выше тростника, о них было сказано в газетах при описании иллюминации, что «город наш украсился, благодаря попечению гражданского правителя, садом.

**15.** Расспросивши подробно будочника, куда можно пройти ближе, если понадобится, к собору, к присутственным местам, к губернатору, он отправился взглянуть на реку, протекавшую посредине города, дорогою оторвал прибитую к столбу афишу, с тем чтобы, пришедши домой, прочитать ее хорошенько, посмотрел пристально на проходившую по деревянному тротуару даму

**16.** Накушавшись чаю, он уселся перед столом, велел подать себе свечу, вынул из кармана афишу, поднес ее к свече и стал читать, прищуря немного правый глаз. Впрочем, замечательного немного было в афишке: давалась драма г. Коцебу, в которой Ролла играл г. Поплёвин, Кору — девица Зяблова, прочие лица были и того менее замечательны.

**17.** Однако же он прочел их всех, добрался даже до цены партера и узнал, что афиша была напечатана в типографии губернского правления, потом переворотил на другую сторону: узнать, нет ли и там чего-нибудь, но, не нашедши ничего, протер глаза, свернул опрятно и положил в свой ларчик, куда имел обыкновение складывать все, что ни попадалось.

**18.** День, кажется, был заключен порцией холодной телятины, бутылкою кислых щей и крепким сном во всю насосную завертку, как выражаются в иных местах обширного русского государства. Весь следующий день посвящен был визитам; приезжий отправился делать визиты всем городским сановникам. Был с почтением у губернатора, который, как оказалось, подобно Чичикову был ни толст, ни тонок собой.

**19.** Потом отправился к вице-губернатору, потом был у прокурора, у председателя палаты, у полицеймейстера, у откупщика, у начальника над казенными фабриками... жаль, что несколько трудно упомнить всех сильных мира сего; но довольно сказать, что приезжий оказал необыкновенную деятельность насчет визитов: он явился даже засвидетельствовать почтение инспектору врачебной управы и городскому архитектору.

**20.** И потом еще долго сидел в бричке, придумывая, кому бы еще отдать визит, да уж больше в городе не нашлось чиновников. В разговорах с сими властителями он очень искусно умел польстить каждому. Губернатору намекнул как-то вскользь, что в его губернию въезжаешь, как в рай, дороги везде бархатные, и что те правительства, которые назначают мудрых сановников, достойны большой похвалы.

Приложение 2.

## Варианты заданий (ключевые фразы)

|  |  |
| --- | --- |
| 1 | Мой дядя самых честных правил,  Когда не в шутку занемог, |
| 2 | Он уважать себя заставил  И лучше выдумать не мог. |
| 3 | Его пример другим наука;  Но, боже мой, какая скука |
| 4 | С больным сидеть и день и ночь,  Не отходя ни шагу прочь! |
| 5 | Какое низкое коварство  Полуживого забавлять, |
| 6 | Ему подушки поправлять,  Печально подносить лекарство, |
| 7 | Вздыхать и думать про себя:  Когда же черт возьмет тебя! |
| 8 | Так думал молодой повеса,  Летя в пыли на почтовых, |
| 9 | Всевышней волею Зевеса  Наследник всех своих родных. |
| 10 | Друзья Людмилы и Руслана!  С героем моего романа |
| 11 | Без предисловий, сей же час  Позвольте познакомить вас: |
| 12 | Онегин, добрый мой приятель,  Родился на брегах Невы, |
| 13 | Где, может быть, родились вы  Или блистали, мой читатель; |
| 14 | Там некогда гулял и я:  Но вреден север для меня. |
| 15 | Служив отлично благородно,  Долгами жил его отец, |
| 16 | Давал три бала ежегодно  И промотался наконец. |
| 17 | Судьба Евгения хранила:  Сперва мадам за ним ходила, |
| 18 | Потом месье ее сменил.  Ребенок был резов, но мил. |
| 19 | Месье Лаббе, француз убогой,  Чтоб не измучилось дитя, |
| 20 | Учил его всему шутя,  Не докучал моралью строгой, |