Практическая работа 2

Часть 1. Задание

Программная реализация симметричного блочного шифра "Кузнечик" (ГОСТ Р 34.12-2015). Программа должна:

1) принимать на вход файл, содержащий открытый текст, подлежащий зашифрованию, или шифртекст, подлежащий расшифрованию; 2) принимать на вход секретный ключ; 3) [дополнительная опция, не являющаяся обязательной] давать пользователю возможность выбирать режим работы блочного шифра; 4) осуществлять зашифрование или расшифрование выбранного файла по выбору пользователя и сохранять результат в новом файле.

Часть 2. Краткая теоретическая часть;

«Кузнечик» (англ. Kuznyechik[1] или англ. Kuznechik[2][3]) — симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 256 бит, использующий для генерации раундовых ключей SP-сеть.

Описание алгоритма. Для шифрования, расшифрования и генерации ключа используются следующие функции: 1) XOR с раундовым ключом 2) Нелинейное биективное преобразование **S** (подстановка по таблице соотвестствия) 3) Линейное преобразование **L**, где происходит сдвиг элементов блока на 1 блок, а утраченный после сдвига блок восполняется путем свертки всех блоков в один в результате линейного преобразования

При зашифровке операции XSL производятся 9 раз (раундов), а 10-й раунд включает только операцию наложения раундового ключа. Расшифрование представляет собой последовательное применение обратных процедур. Подборнее алогитм описывается в Части 3.

Часть 3. Описание программной реализации

Часть 3.1 Описание блочного шифра Кузнечик

Программа реализована в классе `Cricket` в файле cricket.py в данном репозитории.

- Статические параметры `pi` и `pi_inv` : Целочисленные массивы, где индекс каждого элемента соответствует значению исходного при биективном нелинейном отображении (X) и обратной опреации (X^{-1}).
- Метод `__init__(self):` Запускается при инициализации класса. Принимает на вход главный ключ (256 bit), запускает генерацию раундовых ключей и сохраняет их в виде упорядоченного массива в параметре объекта `self.round_keys`
- Статический метод `__generate_round_keys(key)` : Принимает на вход главный 256 битный ключ и генерирует из него 10 раундовых 128 битных ключей.

а) На первом метод разбивает глвный ключ на две равные части, и сохраняет их в массив `self.round_keys` в качестве первых двух ключей.

б) Остальные 8 (4 пары) ключей вырабатываются в цикле `for i in range(4):` , где на каждом шаге цикла к предыдущей паре ключей 8-кратно применяются преобразования сети Фейстеля.

- Метод `encrypt(self, x)` : Принимая на вход блок длинной 128 бит, затем в цикле `for rnd in range(9):` выполняет 9 раундов зашифрования.

  а) Запускает сначала операцию **X** (XOR) с райндовым ключом

  ```
  x ^ self.round_keys[rnd]
  ```

  б) Затем нелинейное биективное преобразование **S**

  ```
  Cricket.__s_transformation(x ^ self.round_keys[rnd])
  ```

  в) И наконец линейное преобразование **L**

  ```
  Cricket.__l_transformation(Cricket.__s_transformation(x ^ self.round_keys[rnd]))
  ```

  где каждый байт 16 раз помножается на соответствующий ему элемент поля Галуа. В программе этот шаг реализован в методе `__linear_function(x)`

  г) Последний, 10 раунд зишифрования является не полным и состоит только из наложения последнего раундового ключа

  ```
  return x ^ self.round_keys[-1]
  ```

- Расшифрование `def decrypt(self, x)` устроено противоположным образом. Метод принимает на вход зашифрованный блок длинной 128 бит.

  а) Сначала строится развернутый массив ключей

  ```
  keys = self.round_keys[::-1]
  ```

  б) Затем 9 раз применяются обратные функции $\mathbf{X^{-1}}$ $\mathbf{S^{-1}}$ $\mathbf{L^{-1}}$

  ```
  x = Cricket.__s_inv_transformation(Cricket.__l_inv_transformation(x ^ keys[rnd]))
  ```

  в) Последний раунд также является не полным и заключается лишьт в применении последнего раундового ключа

  ```
  return x ^ keys[-1]
  ```

Часть 3.2 Описание режимов работы

Режимы реализованы в классе `EncryptionMode` . На момент составления отчета успел реализовать только метод простой подстановки (в методе `ecb_mode`) и метод гаммирования (`ctr_mode`)

- В режиме `ecb_mode` блоки открытого текста напрямую шифруются шифром Кузнечик.

  Размер блока всегда 16 байт (128 бит) `block_size = 16`

  Статический метод `__padding_bytes` сначал добавляет 1 (b'\x01'), а затем нулями добивает количество байт до кратного 16-ти

  Шифрования блоков происходит последовательно и независимо друг от друга, поэтому в шифртекст переносятся статистические характеристики исходного текста, а значит этот шифр является не надежным

- В режиме Гаммирования шифрование происходит не напрямую. Вместо открытого текста алгоритм блочного шифра шифрует счетчик, состоящий из синхропосылки и нулей (на первом этапе), а затем усекается на заданное количество байт. В моей реализации я по умолчанию задаю размер блока 13 байт `block_size: int = 13` , но оно может быть изменено при вызове функции.

  Гамма считается как результат шифрования счетчика, а затьем усечается на заданное количество байт `gamma = cricket.encrypt(counter) >> right_shift`

  Потом я увеличиваю счетчик `counter = EncryptionMode.__increment_counter(counter)`

  И накладываю полученную гамму на блоки открытого текста `encrypted_block = gamma ^ block_int`

  В конце конкатенирую полученные данные к коллекции `result_bytes.extend(encrypted_block)`

  Метод `__get_counter` генерирует счетчик (размером 128 бит) из синхнопосылки и нулей

  Метод `__increment_counter` очевидно служит для увеличения значения счетчика по мере шифрования.

  Расшифрование происходит точно также, за исключением: того что на первом этапе нужно отделить синхропосылку и переопределить счетчик, а также удалить нулевые байты в конце до единичного байта (включительно)

Часть 4. Демонстрация работы программы

1) Чтобы запустить код выполните следующие действия:

`evgeny@hp:~/cricket$ python3 cricket.py <command> <mode> <path/to/file> <key>` , где:

`<command>` - *--encrypt* - чтобы зашифровать файл, *--decrypt* - чтобы расшифровать

`<mode>` - режим шифрования / расшифрования (--dummy / --counter)

`<path/to/file>` - путь к файлу. При зашифровании имя зашифрованного файла будет содержать дополнительное расширение `.enc` . При расшифровании - данное расширение, если оно имеется, будет удалено

`<key>` - 256-битный ключ в виде строки

In [1]:
```
# Выведем на консоль все файлы текущей директории
!ls -l
```

```
total 80
-rwxrwxr-x 1 evgeny evgeny 15667 Mar 24 21:21 cricket.py
-rw-rw-r-- 1 evgeny evgeny     0 Mar 24 20:50 Readme.md
-rw-rw-r-- 1 evgeny evgeny 49555 Mar 24 21:56 report.ipynb
-rw-rw-r-- 1 evgeny evgeny  3302 Mar 24 20:36 test.txt
-rw-rw-r-- 1 evgeny evgeny  3323 Mar 24 21:52 test.txt.cricket
-rw-rw-r-- 1 evgeny evgeny  3302 Mar 24 21:52 test.txt.decrypted
```

In [2]:
```
# Запускаем зашифрование файла test.txt
!./cricket.py --encrypt --dummy "test.txt" "8899aabbccddeeff0011223344556677fe
```

In [3]:
```
!ls -l
```

```
total 80
-rwxrwxr-x 1 evgeny evgeny 15667 Mar 24 21:21 cricket.py
-rw-rw-r-- 1 evgeny evgeny     0 Mar 24 20:50 Readme.md
-rw-rw-r-- 1 evgeny evgeny 49555 Mar 24 21:56 report.ipynb
-rw-rw-r-- 1 evgeny evgeny  3302 Mar 24 20:36 test.txt
-rw-rw-r-- 1 evgeny evgeny  3312 Mar 24 21:57 test.txt.cricket
-rw-rw-r-- 1 evgeny evgeny  3302 Mar 24 21:52 test.txt.decrypted
```

In [4]:
```
# Зашифрованный файл
!cat test.txt.cricket
```

<U@G@4'@@vHW[L@Ķ@@.@@@@▷C@@bx@@/_%¤◁-@@k@@M@@E@@Br^~♂@@@~o@>@{c∝l3:0@@-r@@G
@"p@@K6⍉{f
h@[@@@3@T@@@@<a@@0▷@@`'@BY⏥@@⍉&@@Y@@@@@@◷U@t⍝i⊛@nQ◁>p,E\@/@i@F@@@H@z¤@@@@@_;
@@@@.:3@◡@h◁☿ϟ@@d@@!◁⍉@1@☎@ᵭ9⌀@@@
J,@W@q@@@<T吳]@7lR(@@@⊛eo|@Km@@z□<@p@@i✓♫@⌀@@@@S@j9@@@@☃}$@@ᐡ@@@@>@x@@@@墎
@∝[@7:@(uu@@✓@e♪H;@@)@.@@nemU@▫@@m.:.@@@h◡@@▷@@@@@✓n◀@Q*@@Y@T◀@⍉@m@@x@@!@r►w@@
@0)G@K@◡@F@&@▷⌀l⌕▫K?@4@K@⌀@@@@U
@@@□D~q⍉@@@P@@@Bĸ@¤@♪@@@@▫ᐡ▷sE]@@⍝⌕@@♀Y@@M7@ @@@@@gS@ə1@@◀▷@@□@□8o@K@24'ѐ
L¨yo✓@@y@@)@Lᐡ@W@@@@Э@G@@"@b@, z)%.@@9!@`3@▷^@6@@ϟ@F0@`@z@C@@@@y@|o@b{@#`@@
@:▷@*à0@rO@.@jj@@@@H@@{y@@+~@@@@ +PP@2@@@o@@ϟ@J8t@@►@@@~i?@K@◡@y5A@f@@FW@@@g
@.@r@C☿@ņN@8☿@@⌕◁zu∝@DN@@@@@@▫@v2>@@@(∝@@@@:@_@P@k@@¯z@@Q@@@@♂@@`D^OTT@$W@|
[.:.@@y@P@$e!@@/@x⊛@@@s@@X⍉.:.-♀@⌀o@@@q<@@!Q@@@@ϟ@n/@@@F>@Q@@@'@@@&@@@@@@@@S@.$@@S⌅
@@@N@@@@∝sϟ@@@D¤@►-@h@,R@Ee⌐@@
@@_@¨@☿`@b¨R@v@@@IX@▷o@@@►@E<]Ki∝⌀@@@8@@@6qU(@►▷.:.@a@ϟ:~@'_@⍉Py$b@@uRT@@c@ 1@J
u@(⌐@@@@◀¨@(☿@彈@7ᐯ@@◁@@j@@@;@p@QP:@☎*@ʜ@m@@☿4A@_q@@@`@r)@=@@♂@p@@@@K@@\,k^
@*@ᐟt7@=◡@.♫n@O`@
4@c7 ◁N0@]J☂K`@@4@☎@2@⍉@B@b:@[" @7@@@ю@@o2@♫5@m@@:`@✓ᐯ@@@☎@b@@@@@@@R
@@@☿@h@⌕-☂Ap'@w@@\f@@US@q@✓@2@ᵤu@♀@pO@@@4⌐@@TX@@S♂q@K@@@@@◀g@@c♫@^@H(@@@@@@@
Y♪☿dT/@@}9G@@4
@@;\ƙ@}@@@s@Δ@.♫⌀@✓@\ʒ@4@@@5@@@@@◡▫♂▷);Oe‾@@Un@#Ð.r@t@4q@@
@)R@
@<@@ !@O◷@@@t@0:@x@K@D☂[+@@¤ᐯ@)@@@O@M@^n@@♪6C#@@@S☂@z@@he@@dv@@@V@✓.@@@@@ᐡ◡@F◡@
@s@Mɥu@oI@_@@C'⊛A@@@¯▷q<@@☿@@3@@z@ʓ@4@@@Fq☂U⌀)@@X,c\@4¿b@Fr◡@⊛ïkXU@@☿h⌕✓@\gV@
T@⌀ʜ@@☎í@r@✓@q|@^@fcf@`@w@∝@^@dl<@@_t @@
<>@@'@@ᐯ@@@,c@▷N♫▫@qXTi@S~V▷@@um.@%@V@@sEG◷@y@hɟᐡ◡@@81N@@@@@!@@@N@@g☿@0ᐯ*@@☂@
#UJ@p☿@@@h@dQ
@p@¬@W☎ @b@@✓Z@@ᐡ◡Co>ᒍ▷f@ᐡ◡@)g@@@.@@G◁ɗác@@@@@a@zl@i@@!@@z@m@N4@>@@@@@p
@`⌕✓@@@@\w@◀@xmN
WNY:@G@PZΔ@*ᐡ◡@□UQ@%@@F@WW@,`%@□ɠ@n@l@S@@@>@
@◡@蠶\A@@@@@N<@@@D♫@<+M♂⌐5☿@.A@e@@h@♪@qᵔ⌕@@e►@t@@◀@ 6@@¤@")☎@⌕@@@膱y@@@9♀F@,6
A@.@@l@:@@□@@@@*@@@@□
@dY@EDϵh@@1◀♀@@@@@2`@@Dϳ%@@@@◡@@ɲ@f@N@@@o)>^@□\W☄♫@y☿|☎JU^@@@ᵉ@l鐲NV@u@2@ㄱ8@
I▷@7ᐡ◡@V(⌕x@@@@F:◀(l@?◁[@"@@=@@@@@@@⌀ᐡ◡U☂[@@0\ᐯ\@Y✓\@˙@♂@@]@.M'►X@e∝◁<\@f8@
{@%/
@@ѡ~@IS}~@c@ɔ@E`)FO@@@Q@¨@@ᵝ@C^@'@@ʟ>@Yz◷xn►@@2F%X))@.@
♫)#ᐯx@@ᨈ*@☎!@☂@@*@À@,▫<$@a@@q@)@8@@@@@MV@T@@IGMI⌀@@@⌐@o9@@"♀I◁@@@p☂

In [5]:
```
# Исходный файл
!cat test.txt
```

I
«Мой дядя самых честных правил,
Когда не в шутку занемог,
Он уважать себя заставил
И лучше выдумать не мог.
Его пример другим наука;
Но, боже мой, какая скука
С больным сидеть и день и ночь,
Не отходя ни шагу прочь!
Какое низкое коварство
Полуживого забавлять,
Ему подушки поправлять,
Печально подносить лекарство,
Вздыхать и думать про себя:
Когда же черт возьмет тебя!»
II
Так думал молодой повеса,
Летя в пыли на почтовых,
Всевышней волею Зевеса
Наследник всех своих родных.
Друзья Людмилы и Руслана!
С героем моего романа
Без предисловий, сей же час
Позвольте познакомить вас:
Онегин, добрый мой приятель,
Родился на брегах Невы,
Где, может быть, родились вы
Или блистали, мой читатель;
Там некогда гулял и я:
Но вреден север для меня 1.
III
Служив отлично благородно,
Долгами жил его отец,
Давал три бала ежегодно
И промотался наконец.
Судьба Евгения хранила:
Сперва Madame за ним ходила,
Потом Monsieur ее сменил.
Ребенок был резов, но мил.
Monsieur l'Abbé, француз убогой,
Чтоб не измучилось дитя,
Учил его всему шутя,
Не докучал моралью строгой,
Слегка за шалости бранил
И в Летний сад гулять водил.
IV
Когда же юности мятежной
Пришла Евгению пора,
Пора надежд и грусти нежной,
Monsieur прогнали со двора.
Вот мой Онегин на свободе;
Острижен по последней моде,
Как dandy 2 лондонский одет —
И наконец увидел свет.
Он по-французски совершенно
Мог изъясняться и писал;
Легко мазурку танцевал
И кланялся непринужденно;
Чего ж вам больше? Свет решил,
Что он умен и очень мил.

```
V
Мы все учились понемногу
Чему-нибудь и как-нибудь,
Так воспитаньем, слава богу,
У нас немудрено блеснуть.
Онегин был по мненью многих
(Судей решительных и строгих)
Ученый малый, но педант:
Имел он счастливый талант
Без принужденья в разговоре
Коснуться до всего слегка,
С ученым видом знатока
Хранить молчанье в важном споре
И возбуждать улыбку дам
Огнем нежданных эпиграмм.
```

In [6]:
```
# Запускаю расшифровку файла
!./cricket.py --decrypt --dummy "test.txt.cricket" "8899aabbccddeeff0011223344
```

In [7]:
```
# Смотрим
!ls -l
```

```
total 80
-rwxrwxr-x 1 evgeny evgeny 15667 Mar 24 21:21 cricket.py
-rw-rw-r-- 1 evgeny evgeny     0 Mar 24 20:50 Readme.md
-rw-rw-r-- 1 evgeny evgeny 49555 Mar 24 21:56 report.ipynb
-rw-rw-r-- 1 evgeny evgeny  3302 Mar 24 20:36 test.txt
-rw-rw-r-- 1 evgeny evgeny  3312 Mar 24 21:57 test.txt.cricket
-rw-rw-r-- 1 evgeny evgeny  3302 Mar 24 21:57 test.txt.decrypted
```

In [8]:
```
!cat test.txt.decrypted
```

I
«Мой дядя самых честных правил,
Когда не в шутку занемог,
Он уважать себя заставил
И лучше выдумать не мог.
Его пример другим наука;
Но, боже мой, какая скука
С больным сидеть и день и ночь,
Не отходя ни шагу прочь!
Какое низкое коварство
Полуживого забавлять,
Ему подушки поправлять,
Печально подносить лекарство,
Вздыхать и думать про себя:
Когда же черт возьмет тебя!»
II
Так думал молодой повеса,
Летя в пыли на почтовых,
Всевышней волею Зевеса
Наследник всех своих родных.
Друзья Людмилы и Руслана!
С героем моего романа
Без предисловий, сей же час
Позвольте познакомить вас:
Онегин, добрый мой приятель,
Родился на брегах Невы,
Где, может быть, родились вы
Или блистали, мой читатель;
Там некогда гулял и я:
Но вреден север для меня 1.
III
Служив отлично благородно,
Долгами жил его отец,
Давал три бала ежегодно
И промотался наконец.
Судьба Евгения хранила:
Сперва Madame за ним ходила,
Потом Monsieur ее сменил.
Ребенок был резов, но мил.
Monsieur l'Abbé, француз убогой,
Чтоб не измучилось дитя,
Учил его всему шутя,
Не докучал моралью строгой,
Слегка за шалости бранил
И в Летний сад гулять водил.
IV
Когда же юности мятежной
Пришла Евгению пора,
Пора надежд и грусти нежной,
Monsieur прогнали со двора.
Вот мой Онегин на свободе;
Острижен по последней моде,
Как dandy 2 лондонский одет —
И наконец увидел свет.
Он по-французски совершенно
Мог изъясняться и писал;
Легко мазурку танцевал
И кланялся непринужденно;
Чего ж вам больше? Свет решил,
Что он умен и очень мил.

```
V
Мы все учились понемногу
Чему-нибудь и как-нибудь,
Так воспитаньем, слава богу,
У нас немудрено блеснуть.
Онегин был по мненью многих
(Судей решительных и строгих)
Ученый малый, но педант:
Имел он счастливый талант
Без принужденья в разговоре
Коснуться до всего слегка,
С ученым видом знатока
Хранить молчанье в важном споре
И возбуждать улыбку дам
Огнем нежданных эпиграмм.
```

In [9]:
```
# Удалю артефакты и вызову с новыми аргументами
!rm -rf test.txt.encrypted test.txt.decrypted
```

In [10]:
```
!./cricket.py --encrypt --control "test.txt" "8899aabbccddeeff0011223344556677
```

In [11]:
```
!./cricket.py --decrypt --control "test.txt.cricket" "8899aabbccddeeff00112233
```

In [12]:
```
!ls -l
```

```
total 64
-rwxrwxr-x 1 evgeny evgeny 15667 Mar 24 21:21 cricket.py
-rw-rw-r-- 1 evgeny evgeny     0 Mar 24 20:50 Readme.md
-rw-rw-r-- 1 evgeny evgeny 35754 Mar 24 21:57 report.ipynb
-rw-rw-r-- 1 evgeny evgeny  3302 Mar 24 20:36 test.txt
-rw-rw-r-- 1 evgeny evgeny  3323 Mar 24 21:57 test.txt.cricket
-rw-rw-r-- 1 evgeny evgeny  3302 Mar 24 21:57 test.txt.decrypted
```

In [13]:
```
!cat test.txt.cricket
```

```
R@k@=@.Xq SPz@ Z@@@@o@¤4@⌐)$^@I@@^@*vn⍑@ϟ
@@⍉@@@p@h@ @azb@@ɘl@@Y@@5@ʃ.@7!A@ _:ju@ɳ.@:⍰:@Ↄs⊵@Lg◄ₐ@ @nVf 90@@j♫♀
►@a@@Q@kQ@@@v@@f@@@♂@@@@A⌀@hs@1@B@)dL@@r@@vnpB@@@n@N⊛@@☎(ڸ@%,@V@.\@g@3@□@⍉|@Y
ᵥs@¨@@P@@@@◁!Ŭ@@⊵⌐@@Kt
@⊵☎r@|/U^`-p@▷&@@@?@ϟ@@H@@@@@u◁7{@
@@@⌕hAo@ @@⌀@@@@⊛@⊵7b\@V@@@Mb@#@@Z@♫@ₐ@@@@C⍭@]@m◁5¤3@a.@@@ZY@@6@>@@ʊP@►@g)Z@
@⊛(|=@H□xx⊵@cx□@N@@♫@9@ʒ@@@.@⌐I@A@@A@@
@<!@@Ti♪ㅍ}~@
_@@f[@ↀ♂@¤a@Qʊ@@R@Fms@ÆQ>♫(~@r@@/@@.@@∴⌀@@i
@▷Wɯ⍉@@.*@@@@?@#@pƒ8@@$^X◁\@ɟ@@h ✓^✓\T@:7⍉✓@@@ !364@@@sB@1O @J@ψ@@@i{@{9@@G
>¤.ɳ@8!@@@∝@u>@@@
@?ψ@!@@ @@;@@@@amE3@9₾@#◁|@@@@W@@@@@2∝=@₾@$
+@R+∝@g@Je5%1@@@@|u@B@p:@@@o@.y,@@/@@@@@@uĉ@!@ₐ@@@<@@@ʊ@!X⊛qq@@@@@@
@▷@5♂@|@f@@Yu&@,EWe@ₓ@Y$@?@s@@N⌕@@@8@
5S@@B@♀=@@@◁4!ᵑ@e@@O@@@ 6ᘯ@dp@Y!@⊵@(c&=►'@✓+◷@@⌕l@Y`@i♀@9@^= da@@ceV◄@@✓Ù@TA
@@N@f►9⊛ϟ@ₐO@@)@@◄@#@C@ℑ.ϟ☎@瑁7@@@e-@Z@@@@@6ɣY@(ʊ@@XQ☎@@⍉@;D'@W@j%`qUO"@◁*L
Q@@{@@@FY@ğI@@a@@R@rd@/◂◱@@@8Z!@@"@'I@@@M@⊵G@@m@@
@X@@⊵@H@p@Rh<b@@@7◄;@
@W⌀Ⱶ‘◄\@ɳ◁@h@]@3ez@Q◁tKi@T@@'.@"N@h@~Q@@t@@5@@@i@◁@5@`J@
+@
f2fR@L^/俵□8@□@@w@
@q¨D⍉ʊ@q@0ҡ@⍉@@@@@@♪@@@i@Ɨ@-@:∴@@☿8ʊ@#mY@Va⌀@N@@ v@&R@’@Fo@@j\@^@@@◁Wqa
@@@@@<<@8@@{@@@♪@|@.几@P~TaU@ëN@@]ᘯÕ@i@n6⍑@@@}@⌕@@@@✓♫@c'@@!@@@G@V⌐MB@@mO⌕].∴@
cmvN@@"@@@@V@@;S@@⊵◱@@C∝uS51@9aLᘯr⌐@R@8@ʌ5b3Sf*@,@@H~⌀@@@@@7_@ZI@☎^@w@6@&@f
B⊛pцg@@@@ˈ$4@$@@@h.∴@^J@@@;@C0@@W☿@@@?@}h@"@@@@@@@@@@@@Nhh@@K3QZ@@St ɹc@⌕@@JO@1
T@ʊ@⍑@p|O@@♀@W⌀@Q=@C@@@-@A @@y@m@o@◁@@-@Gb@@S@@@aQ∝@@@z@.∴Nfk25m@@цJ@z@@@
@⍑@$@Vṭ@z@!V@@-a@x@A@@@@⌀U@@$W@@@e♫oA@
@◁z@@✓u!@\@@g@@@-
@tb◷@@*@ϟM◄ƀTot@◷{@@@@>Au@ck@}e@d@@@t5{y@@f@-6@@o,@∝@@⌀@@@@<Sn@<@@H☿@✓@@@
\@.ᘯ¤@@@}@`@@@@H@>at2ʊ◄4@@\@@@e@@U@ɲxd◄/⊵@☿4(⌕@@or@⍉♫@$@@`_q♀@9a@@@Q@t@@c
@✓q
K~/@@@O☎¤oH@fY@z7B@@⍑♂@@v@[}@ x@@/@@@tV@@@@Bw@ᘯ◁@@@t@@@c@@+@@t@@~@@@@@;/@
@.¿►@⌕a2@@@eU@j@)?@p@@@3@@@►O@#@Ii@PJ¸@@p@@@✓⌀7@FIʊKγA@►@ᘯc∝oN⍉@T^ᵕ@@@⊵?
v@@@Q@C∴▷@pD@TG@Ă@$⍑(X`{gz@@@ϟ@ʊ@@@♂@*@@@t@n@v◁@#E;。|@@0⌀^B@@◄[@@@@@@@<m\/@@
@ORxW⁒@@DI@@6@A∝⍉@@!@@;@@o@@<3@a@₾@ʊ@.∴◄@@z@"@@?◁@@@@⍉n@✓V@@E@@c@p∴,7¸i@@@I@v`
V☎@@=@mxO`9.∴@&M5N@⊛⍉@&G♀@n @;WV!@@Y@@⌐@b.c@V@@⍉@@@TG3@♪@@@@H: ϟ@@@j@@∝@@@@@_
l@@@a@7@Ⱨ@o7@;@@@◄@ @.@@^⌕@⌐CĘ@;.
Gɳ@}i@,@♫@@@@и@☿@"@U
```

In [14]:

```
!cat test.txt.decrypted
```

I
«Мой дядя самых честных правил,
Когда не в шутку занемог,
Он уважать себя заставил
И лучше выдумать не мог.
Его пример другим наука;
Но, боже мой, какая скука
С больным сидеть и день и ночь,
Не отходя ни шагу прочь!
Какое низкое коварство
Полуживого забавлять,
Ему подушки поправлять,
Печально подносить лекарство,
Вздыхать и думать про себя:
Когда же черт возьмет тебя!»
II
Так думал молодой повеса,
Летя в пыли на почтовых,
Всевышней волею Зевеса
Наследник всех своих родных.
Друзья Людмилы и Руслана!
С героем моего романа
Без предисловий, сей же час
Позвольте познакомить вас:
Онегин, добрый мой приятель,
Родился на брегах Невы,
Где, может быть, родились вы
Или блистали, мой читатель;
Там некогда гулял и я:
Но вреден север для меня 1.
III
Служив отлично благородно,
Долгами жил его отец,
Давал три бала ежегодно
И промотался наконец.
Судьба Евгения хранила:
Сперва Madame за ним ходила,
Потом Monsieur ее сменил.
Ребенок был резов, но мил.
Monsieur l'Abbé, француз убогой,
Чтоб не измучилось дитя,
Учил его всему шутя,
Не докучал моралью строгой,
Слегка за шалости бранил
И в Летний сад гулять водил.
IV
Когда же юности мятежной
Пришла Евгению пора,
Пора надежд и грусти нежной,
Monsieur прогнали со двора.
Вот мой Онегин на свободе;
Острижен по последней моде,
Как dandy 2 лондонский одет —
И наконец увидел свет.
Он по-французски совершенно
Мог изъясняться и писал;
Легко мазурку танцевал
И кланялся непринужденно;
Чего ж вам больше? Свет решил,
Что он умен и очень мил.

```
V
Мы все учились понемногу
Чему-нибудь и как-нибудь,
Так воспитаньем, слава богу,
У нас немудрено блеснуть.
Онегин был по мненью многих
(Судей решительных и строгих)
Ученый малый, но педант:
Имел он счастливый талант
Без принужденья в разговоре
Коснуться до всего слегка,
С ученым видом знатока
Хранить молчанье в важном споре
И возбуждать улыбку дам
Огнем нежданных эпиграмм.
```

Спасибо за внимание и да пребудет с вами сила!

С уважением, Шараев Евгений!