Часть 4 Демонстрация

Часть 4.1 Демонстрация работы блочного шифра Кузнечик

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]:
```
# Демонстрация работы блочного шифра Кузнечик
# импорт классов
from cricket import Cricket

# Создам объект класса Cricket и передам ему 256-битный ключ
cricket = Cricket("8899aabbccddeeff0011223344556677fedcba9876543210012
# Объект класса готов к работе
cricket
```

Out[1]:
```
<cricket.Cricket at 0x7c9743136950>
```

In [2]:
```
# Блочный шифр Кузнечик выполняет 10 раундов шифрования и для каждого
# Раундовые ключи генерируются при инициализации объекта и их можно "п

cricket.round_keys
```

Out[2]:
```
[181572891734806641530322838679085999735,
 338770000845734292516042252062085074415,
 291356820539020174378226036445198912580,
 814428768517603488548074600570961257 00,
 116164101860579397447240808000140210604,
 251263443283993162038968266093410015259,
 108863003319109490105301954974994962609,
 120259538107168560546004230169145309572,
 248923301836046559943424202620957811991,
 152746288297545385236998257316467458115]
```

In [3]:
```
# Случайная строка для демонстрации работы класса
string = "qB!5pZ@7#tC2*dXe".encode()

# Длинная строки 16 байт - 128 бит
print(len(string))

# Метод encrypt принимает данные в виде целочисленных значений
string_int = int.from_bytes(string, byteorder="big")
encrypted = cricket.encrypt(string_int)
encrypted_bytes = int.to_bytes(encrypted, 16, byteorder="big")

# Зашифрованные текст
print(encrypted_bytes)

# Расшифровываем обратно
decrypted = cricket.decrypt(encrypted)
decrypted_bytes = int.to_bytes(decrypted, 16, byteorder="big")
print(decrypted_bytes)

# Проверка на правильность
assert decrypted_bytes == string

print("Assert: [OK]")
```

```
16
b'"\x1f\xf2F3G\x92vS\x89\xe7Ir\xef\xa32'
b'qB!5pZ@7#tC2*dXe'
Assert: [OK]
```

Часть 4.2 Демонстрация работы режимов шифрования

4.2.1 Режим простой замены

In [4]:
```
# Выведем на консоль все файлы текущей директории
# Вы видите 5 тестовых файлов с разными отрвыками знаменитой поэмы
!ls -l
```

```
total 828
-rwxrwxr-x 1 evgeny evgeny  25651 Mar 27 14:17 cricket.py
-rw-rw-r-- 1 evgeny evgeny  35940 Mar 27 15:15 demo.ipynb
drwxrwxr-x 2 evgeny evgeny   4096 Mar 27 14:28 __pycache__
-rw-rw-r-- 1 evgeny evgeny      0 Mar 24 20:50 Readme.md
-rw-rw-r-- 1 evgeny evgeny 754168 Mar 24 23:21 sharaev_evgeny_report_
pr_2.pdf
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 14:22 test_part1.txt
-rw-rw-r-- 1 evgeny evgeny    660 Mar 27 14:22 test_part2.txt
-rw-rw-r-- 1 evgeny evgeny    629 Mar 27 14:22 test_part3.txt
-rw-rw-r-- 1 evgeny evgeny    655 Mar 27 14:22 test_part4.txt
-rw-rw-r-- 1 evgeny evgeny    683 Mar 27 14:22 test_part5.txt
```

In [5]:
```
# Запускаем зашифрование файла test_part1.txt в режиме простой замены
!./cricket.py --encrypt --dummy "test_part1.txt" "8899aabbccddeeff0011
```

In [6]:
```
# Видим что появился файл test_part1.txt.cricket - результат работы
!ls -l
```

```
total 832
-rwxrwxr-x 1 evgeny evgeny  25651 Mar 27 14:17 cricket.py
-rw-rw-r-- 1 evgeny evgeny  35940 Mar 27 15:15 demo.ipynb
drwxrwxr-x 2 evgeny evgeny   4096 Mar 27 14:28 __pycache__
-rw-rw-r-- 1 evgeny evgeny      0 Mar 24 20:50 Readme.md
-rw-rw-r-- 1 evgeny evgeny 754168 Mar 24 23:21 sharaev_evgeny_report_
pr_2.pdf
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 14:22 test_part1.txt
-rw-rw-r-- 1 evgeny evgeny    672 Mar 27 15:15 test_part1.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    660 Mar 27 14:22 test_part2.txt
-rw-rw-r-- 1 evgeny evgeny    629 Mar 27 14:22 test_part3.txt
-rw-rw-r-- 1 evgeny evgeny    655 Mar 27 14:22 test_part4.txt
-rw-rw-r-- 1 evgeny evgeny    683 Mar 27 14:22 test_part5.txt
```

In [7]:
```
# Попробуем прочитать зашифрованный файл
!cat test_part1.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◁⊀↯@@d@@!◁⍉@1@☎@ᵭ9⌀@@@
J,@W@q@@@<T旲]@7lR(@@@⊛eo|@Km@@z□<@p@@♫@⌀@@@@S@j9@@@@₍}$@@ᕑ@@@@>@x@@
@@墲@∝[@7:@(uu@@e♪H;@@)@.@@nemU@ₙ@@m.⁚.@@@hᕑ@@≥@@@@n◄@Q*@@Y@T◄@⍉@m@@x@
@!@r►w@@@0)G@K@ᕑ@F@&@≥⌀l⌕ₙK?@4@K@⌀@@@@U
@@@□D~q⍉@@@P@@@Bₖ@¤@♪@@@@@ₓᛉ▷sE]@@⍝@@♀Y@@M7@  @@@@@gS@ə1@@◄≥@@□@□8
o@K@24'è>@L@@J@@5@ᕑ@@)@c
```

In [8]:
```
# Расшифруем файл в режиме простой замены
!./cricket.py --decrypt --dummy "test_part1.txt.cricket" "8899aabbccdd
```

In [9]:
```
# Видим что появился файл test_part1.txt.decrypted - результат работы
!ls -l
```

```
total 836
-rwxrwxr-x 1 evgeny evgeny  25651 Mar 27 14:17 cricket.py
-rw-rw-r-- 1 evgeny evgeny  35940 Mar 27 15:15 demo.ipynb
drwxrwxr-x 2 evgeny evgeny   4096 Mar 27 14:28 __pycache__
-rw-rw-r-- 1 evgeny evgeny      0 Mar 24 20:50 Readme.md
-rw-rw-r-- 1 evgeny evgeny 754168 Mar 24 23:21 sharaev_evgeny_report_
pr_2.pdf
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 14:22 test_part1.txt
-rw-rw-r-- 1 evgeny evgeny    672 Mar 27 15:15 test_part1.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 15:15 test_part1.txt.decrypt
ed
-rw-rw-r-- 1 evgeny evgeny    660 Mar 27 14:22 test_part2.txt
-rw-rw-r-- 1 evgeny evgeny    629 Mar 27 14:22 test_part3.txt
-rw-rw-r-- 1 evgeny evgeny    655 Mar 27 14:22 test_part4.txt
-rw-rw-r-- 1 evgeny evgeny    683 Mar 27 14:22 test_part5.txt
```

In [10]:
```
# Попробуем прочитать расшифрованный файл
!cat test_part1.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!»
```

4.2.2 Режим простой замены с зацеплением

In [11]:
```
!./cricket.py --encrypt --cbc_mode "test_part2.txt" "8899aabbccddeeff0
```

In [12]:
```
# Видим что появился файл test_part2.txt.cricket - результат работы
!ls -l
```

```
total 840
-rwxrwxr-x 1 evgeny evgeny  25651 Mar 27 14:17 cricket.py
-rw-rw-r-- 1 evgeny evgeny  35940 Mar 27 15:15 demo.ipynb
drwxrwxr-x 2 evgeny evgeny   4096 Mar 27 14:28 __pycache__
-rw-rw-r-- 1 evgeny evgeny      0 Mar 24 20:50 Readme.md
-rw-rw-r-- 1 evgeny evgeny 754168 Mar 24 23:21 sharaev_evgeny_report_
pr_2.pdf
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 14:22 test_part1.txt
-rw-rw-r-- 1 evgeny evgeny    672 Mar 27 15:15 test_part1.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 15:15 test_part1.txt.decrypt
ed
-rw-rw-r-- 1 evgeny evgeny    660 Mar 27 14:22 test_part2.txt
-rw-rw-r-- 1 evgeny evgeny    704 Mar 27 15:15 test_part2.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    629 Mar 27 14:22 test_part3.txt
-rw-rw-r-- 1 evgeny evgeny    655 Mar 27 14:22 test_part4.txt
-rw-rw-r-- 1 evgeny evgeny    683 Mar 27 14:22 test_part5.txt
```

In [13]:
```
# Попробуем прочитать зашифрованный файл
!cat test_part2.txt.cricket
```

```
h u ►9?-A >  ~     ~     ◷   N♪VK  gn Q≤  ~ ;|∓/   v+5♂  sA
6-  ☼  lu<ϟ∝ :.! ►  Q  I Z'a0 z   '  $,\IA B  s♪q@  Wk {Ä       6 =
@♀  Y uPJ wyc k[  ~`  | `y  8   p b r ╪ ♀ ʇC  ☎h ∝H  ☼ b e   ₀ ▷ k;>
o@   `  =  gH  9  T% 9y◁♂ F!   ₀r8t;.▷b5       nϙ    vY  }  i ≥0
v1{5ʖM    L♫ ♂ /WqF ⌐ * ₀ !ϒ  QJ
```

In [14]:
```
!./cricket.py --decrypt --cbc_mode "test_part2.txt.cricket" "8899aabbc
```

In [15]:
```
# Попробуем прочитать расшифрованный файл
!cat test_part2.txt.decrypted
```

```
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.
```

4.2.3 Режим гаммирования

In [16]:
```
!./cricket.py --encrypt --ctr_mode "test_part3.txt" "8899aabbccddeeff0
```

In [17]:
```
# Видим что появился файл test_part3.txt.cricket - результат работы
!ls -l
```

```
total 848
-rwxrwxr-x 1 evgeny evgeny  25651 Mar 27 14:17 cricket.py
-rw-rw-r-- 1 evgeny evgeny  35940 Mar 27 15:15 demo.ipynb
drwxrwxr-x 2 evgeny evgeny   4096 Mar 27 14:28 __pycache__
-rw-rw-r-- 1 evgeny evgeny      0 Mar 24 20:50 Readme.md
-rw-rw-r-- 1 evgeny evgeny 754168 Mar 24 23:21 sharaev_evgeny_report_
pr_2.pdf
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 14:22 test_part1.txt
-rw-rw-r-- 1 evgeny evgeny    672 Mar 27 15:15 test_part1.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 15:15 test_part1.txt.decrypt
ed
-rw-rw-r-- 1 evgeny evgeny    660 Mar 27 14:22 test_part2.txt
-rw-rw-r-- 1 evgeny evgeny    704 Mar 27 15:15 test_part2.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    660 Mar 27 15:15 test_part2.txt.decrypt
ed
-rw-rw-r-- 1 evgeny evgeny    629 Mar 27 14:22 test_part3.txt
-rw-rw-r-- 1 evgeny evgeny    645 Mar 27 15:15 test_part3.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    655 Mar 27 14:22 test_part4.txt
-rw-rw-r-- 1 evgeny evgeny    683 Mar 27 14:22 test_part5.txt
```

In [18]:
```
# Попробуем прочитать зашифрованный файл
!cat test_part3.txt.cricket
```

```
¤(!t@⊛ᔓ@@X@@@Q◃3rف☎Q@◃HY?N@
@]U=@@@mY@@yg@@Q@⍉@@$oa@=@S@⌕ @@@◂@@ᔕb@x@J@7@@@<!
@ᵀ@ʰ@:@nᵛ]@@@3@@M@@Mc@W@A7@@R"'Ç@@f◁?@@⌐;@◡@Q►@@@&@ᵩ_@/◷@@c@@@¤@p|@
X@e◷a@)⌕@♂@@"kᔓ@>⌕@@@j@@@?r@@Y@ᴗ0~~@◃□□F@@8◁@@@&@v6(_@<@R毀@
@R@@♫@O@lʏfᵵ@@ᵀ@@@x|d~!@@@.⁚3@@@@⊛@@@ᵩ@@@W@;u@`@Ta@V@&@7h♫@S@2@iE@z@p
@"@@@@@wT@♫-@^@@N@⌕d@@@F@7a@UG@t@/@?@∝E`;@]@H+@zK@"_@:@@U$H@l@@ϟC☎
ΓЂ @@t5@wb@q@sP+@q@?@H@@@@@#@.t@⊛@j⊛ϟ@@@o@U@@◃@a0"Sᵩcx%@@[¤+y;
@ŷ♪r@;@]:X@@@*@@@gWf<☎@ᴗ{@DŽ[@@)@@ᶎ⊛@JsX|8@@@O▷q@@@@@@>ٹ录b2O2♫@@≥^0
~@@5
```

In [19]:
```
!./cricket.py --decrypt --ctr_mode "test_part3.txt.cricket" "8899aabbc
```

In [20]:
```
# Попробуем прочитать зашифрованный файл
!cat test_part3.txt.decrypted
```

```
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.
```

4.2.4 Режим гаммирования с обратной связью по выходу

In [21]:
```
!./cricket.py --encrypt --ofb_mode "test_part4.txt" "8899aabbccddeeff0
```

In [22]:
```
# Видим что появился файл test_part4.txt.cricket - результат работы
!ls -l
```

```
total 856
-rwxrwxr-x 1 evgeny evgeny  25651 Mar 27 14:17 cricket.py
-rw-rw-r-- 1 evgeny evgeny  35940 Mar 27 15:15 demo.ipynb
drwxrwxr-x 2 evgeny evgeny   4096 Mar 27 14:28 __pycache__
-rw-rw-r-- 1 evgeny evgeny      0 Mar 24 20:50 Readme.md
-rw-rw-r-- 1 evgeny evgeny 754168 Mar 24 23:21 sharaev_evgeny_report_
pr_2.pdf
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 14:22 test_part1.txt
-rw-rw-r-- 1 evgeny evgeny    672 Mar 27 15:15 test_part1.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 15:15 test_part1.txt.decrypt
ed
-rw-rw-r-- 1 evgeny evgeny    660 Mar 27 14:22 test_part2.txt
-rw-rw-r-- 1 evgeny evgeny    704 Mar 27 15:15 test_part2.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    660 Mar 27 15:15 test_part2.txt.decrypt
ed
-rw-rw-r-- 1 evgeny evgeny    629 Mar 27 14:22 test_part3.txt
-rw-rw-r-- 1 evgeny evgeny    645 Mar 27 15:15 test_part3.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    629 Mar 27 15:15 test_part3.txt.decrypt
ed
-rw-rw-r-- 1 evgeny evgeny    655 Mar 27 14:22 test_part4.txt
-rw-rw-r-- 1 evgeny evgeny    695 Mar 27 15:15 test_part4.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    683 Mar 27 14:22 test_part5.txt
```

In [23]:
```
# Попробуем прочитать зашифрованный файл
!cat test_part4.txt.cricket
```

```
[illegible]
```

In [24]:
```
!./cricket.py --decrypt --ofb_mode "test_part4.txt.cricket" "8899aabbc
```

In [25]:
```
# Попробуем прочитать зашифрованный файл
!cat test_part4.txt.decrypted
```

```
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.
```

4.2.5 Режим гаммирования с обратной связью по шифртексту

In [26]:
```
!./cricket.py --encrypt --cfb_mode "test_part5.txt" "8899aabbccddeeff0
```

In [27]:
```
# Видим что появился файл test_part5.txt.cricket - результат работы
!ls -l
```

```
total 864
-rwxrwxr-x 1 evgeny evgeny  25651 Mar 27 14:17 cricket.py
-rw-rw-r-- 1 evgeny evgeny  35940 Mar 27 15:15 demo.ipynb
drwxrwxr-x 2 evgeny evgeny   4096 Mar 27 14:28 __pycache__
-rw-rw-r-- 1 evgeny evgeny      0 Mar 24 20:50 Readme.md
-rw-rw-r-- 1 evgeny evgeny 754168 Mar 24 23:21 sharaev_evgeny_report_
pr_2.pdf
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 14:22 test_part1.txt
-rw-rw-r-- 1 evgeny evgeny    672 Mar 27 15:15 test_part1.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    671 Mar 27 15:15 test_part1.txt.decrypt
ed
-rw-rw-r-- 1 evgeny evgeny    660 Mar 27 14:22 test_part2.txt
-rw-rw-r-- 1 evgeny evgeny    704 Mar 27 15:15 test_part2.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    660 Mar 27 15:15 test_part2.txt.decrypt
ed
-rw-rw-r-- 1 evgeny evgeny    629 Mar 27 14:22 test_part3.txt
-rw-rw-r-- 1 evgeny evgeny    645 Mar 27 15:15 test_part3.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    629 Mar 27 15:15 test_part3.txt.decrypt
ed
-rw-rw-r-- 1 evgeny evgeny    655 Mar 27 14:22 test_part4.txt
-rw-rw-r-- 1 evgeny evgeny    695 Mar 27 15:15 test_part4.txt.cricket
-rw-rw-r-- 1 evgeny evgeny    655 Mar 27 15:15 test_part4.txt.decrypt
ed
-rw-rw-r-- 1 evgeny evgeny    683 Mar 27 14:22 test_part5.txt
-rw-rw-r-- 1 evgeny evgeny    720 Mar 27 15:15 test_part5.txt.cricket
```

In [28]:
```
!./cricket.py --decrypt --cfb_mode "test_part5.txt.cricket" "8899aabbc
```

In [29]:
```
# Попробуем прочитать зашифрованный файл
!cat test_part5.txt.decrypted
```

```
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!