

Министерство образования и науки Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение высшего  
образования

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»  
(МОСКОВСКИЙ ПОЛИТЕХ)**

**ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**КАФЕДРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

**Программирование криптографических алгоритмов**

**Блок Е: Шифры гаммирования**

**Выполнила студентка 3 курса группы 171-341**

**Решетникова Дарья**

**Москва 2020 г.**

## Аннотация

**Язык :** Python

**Программа:** Visual Studio 2017

**Пословица:** Плод никогда не падает далеко от дерева.

**Текст:** История, как и любая учебная дисциплина, имеет свой объект и предмет исследования. Объектом исследования является исторический процесс - последовательный процесс развития природы и общества, череда сменяющих друг друга событий, в которых проявляется деятельность многих поколений людей. С каждым мгновением времени, ушедшим в прошлое исторический процесс дополняется совокупностью новых событий, явлений, фактов и факторов в жизни человека, семьи, этноса, государства, человечества. Подобно тому, как материальный мир переживает процессы негэнтропии и энтропии, природа вокруг нас - процессы эволюции и инволюции, человеческое общество характеризуют процессы социального прогресса и регресса. Предметом изучения истории является деятельность главного его субъекта - человека - в прошлом. В узком смысле история представляет собой совокупность социальных фактов, знаний, представлений ученых о том, как эти процессы осуществлялись и осуществляются. Долгое время история существовала скорее, как литература и искусство, обслуживающие интересы власти, нежели наука. Не случайно в греческой мифологии в свите античного бога Аполлона, покровителя искусств и наук, среди других муз была Клио - муза истории.

### SEO-АНАЛИЗ ТЕКСТА

FAQ API проверки

История, как и любая учебная дисциплина, имеет свой объект и предмет исследования. Объектом исследования является исторический процесс - последовательный процесс развития природы и общества, череда сменяющих друг друга событий, в которых проявляется деятельность многих поколений людей. С каждым мгновением времени, ушедшим в прошлое исторический процесс дополняется совокупностью новых событий, явлений, фактов и факторов в жизни человека, семьи, этноса, государства, человечества. Подобно тому, как материальный мир переживает процессы негэнтропии и энтропии, природа вокруг нас - процессы эволюции и инволюции, человеческое общество характеризуют процессы социального прогресса и регресса. Предметом изучения истории является деятельность главного его субъекта - человека - в прошлом. В узком смысле история представляет собой совокупность социальных фактов, знаний, представлений ученых о том, как эти процессы осуществлялись и осуществляются. Долгое время история существовала скорее, как литература и искусство, обслуживающие интересы власти, нежели наука. Не случайно в греческой мифологии в свите античного бога Аполлона, покровителя искусств и наук, среди других муз была Клио - муза истории.

Всего символов: 1190    Без пробелов: 1042    Количество слов: 149

Заказать текст

Проверить SEO-данные

## Одноразовый блокнот К.Шеннона.

### 1. Описание шифра.

Популярность поточных шифров обязана анализу одноразовых гамма-блокнотов Клода Шеннона. Название «одноразовый блокнот» стало общепринятым в годы Второй мировой войны, когда для шифрования широко использовались бумажные блокноты.

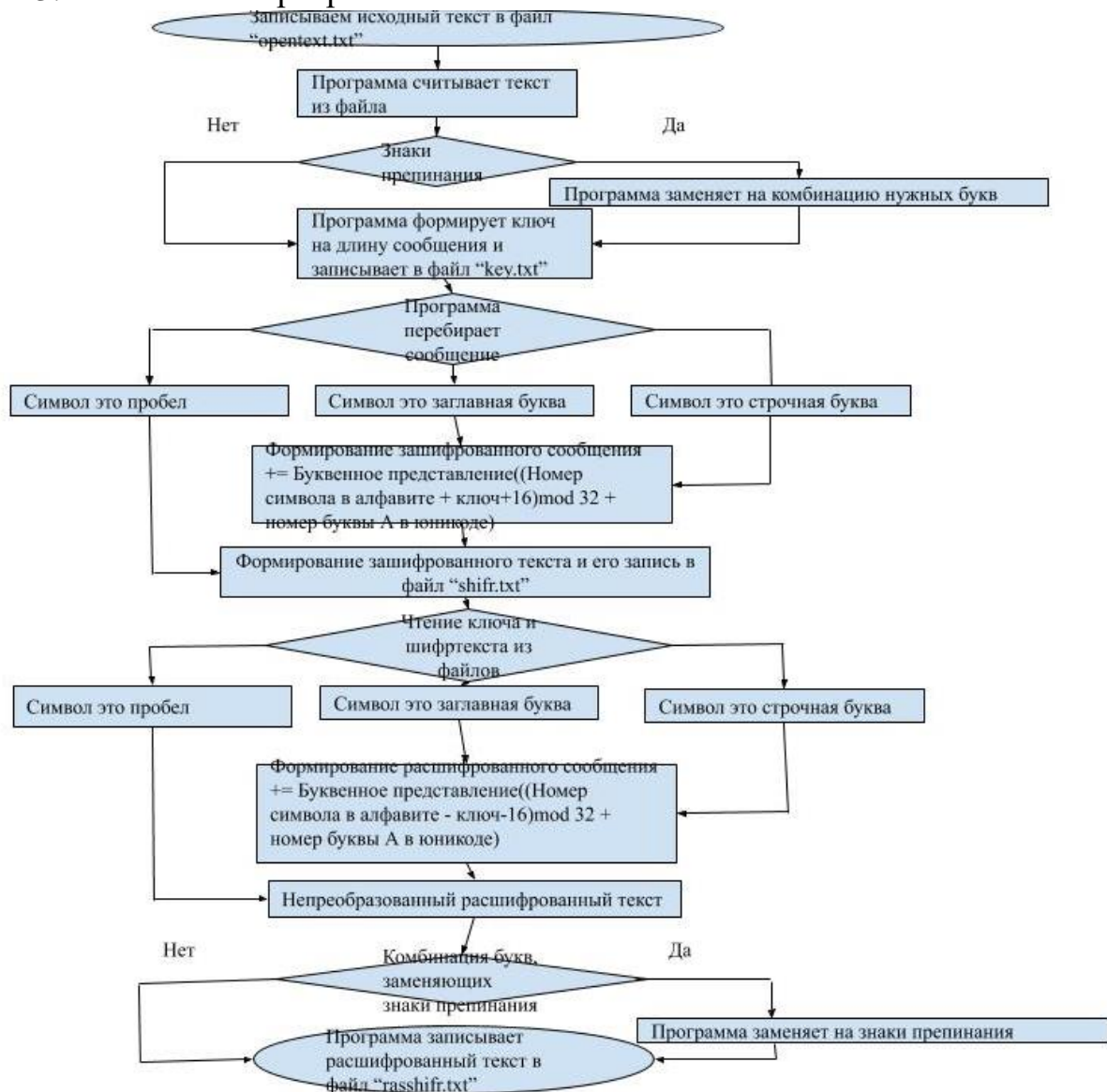
### 2. Алгоритм шифра.

Открытый текст сообщения  $m$  записывают, как последовательность бит или символов  $m = m_0m_1\dots m_{n-1}$ , а двоичную или символьную шифрующую последовательность  $k$  той же самой длины — как  $k = k_0k_1\dots k_{n-1}$ .

Шифртекст  $c = c_0c_1\dots c_{n-1}$  определяется соотношением  $c_i = m_i \oplus k_i$  при  $0 \leq i \leq n-1$ , где  $\oplus$  обозначает операцию «исключающее ИЛИ» (ассемблерная операция XOR) по модулю два или по любому другому модулю в случае символьной гаммы.

В своей исторической работе «Communication theory of secrecy systems» («Теория связи в секретных системах», 1949г.) Шеннон доказал то, что **одноразовый гамма-блокнот является «невскрываемой» шифрсистемой.**

### 3. Блок-схема программы



## 4. Код программы

```
from random import randint
# Функция зашифрования
def encryptShannon(mes):
    mes = mes.replace('.', ' тчк') # Если в сообщении попадетс я точка, она заменется
на тчк
    mes = mes.replace(',', ' зпт') # Если в сообщении попадетс я запятая, она заменется
на зпт
    mes = mes.replace('-', 'тире') # Если в сообщении попадетс я - (тире), оно
заменется на тире
    key = ''
    keys = ''
    final = ''
    llst =
['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', '
х', 'ц', 'ч', 'ш', 'щ', 'ь', 'ы', 'ь', 'э', 'ю', 'я'] # задаем алфавит строчных букв
    blst =
['А', 'Б', 'В', 'Г', 'Д', 'Е', 'Ж', 'З', 'И', 'Й', 'К', 'Л', 'М', 'Н', 'О', 'П', 'Р', 'С', 'Т', 'У', 'Ф', '
Х', 'Ц', 'Ч', 'Ш', 'Щ', 'Ь', 'Ы', 'Ь', 'Э', 'Ю', 'Я'] # задаем алфавит заглавных букв
    for symbol in mes:
        key = randint(0,31)
        keys += str(key) + "/"
        if symbol != " " and symbol in blst:
            final += chr((ord(symbol) + key - 16)%32 + ord('А'))
        elif symbol != " " and symbol in llst:
            final += chr((ord(symbol) + key - 16)%32 + ord('а'))
        else:
            final += " "
    fk = open('key.txt', 'w', encoding='utf-8') # открываем документ key.txt
    fk.write(keys) # записываем туда ключ
    print ('Ключ шифрования: ', keys)
    return final
# Функция расшифрования
def decryptShannon(final):
    fk = open('key.txt', 'r', encoding='utf-8') # открываем документ key.txt
    keys = fk.read() # считываем оттуда key - весь ключ
    keys = keys.split('/')
    mes = ''
    llst =
['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', '
х', 'ц', 'ч', 'ш', 'щ', 'ь', 'ы', 'ь', 'э', 'ю', 'я'] # задаем алфавит строчных букв
    blst =
['А', 'Б', 'В', 'Г', 'Д', 'Е', 'Ж', 'З', 'И', 'Й', 'К', 'Л', 'М', 'Н', 'О', 'П', 'Р', 'С', 'Т', 'У', 'Ф', '
Х', 'Ц', 'Ч', 'Ш', 'Щ', 'Ь', 'Ы', 'Ь', 'Э', 'Ю', 'Я'] # задаем алфавит заглавных букв
    for i, symbol in enumerate(final):
        if symbol != " " and symbol in blst:
            mes += chr((ord(symbol) - int(keys[i]) - 16)%32 + ord('А'))
        elif symbol != " " and symbol in llst:
            mes += chr((ord(symbol) - int(keys[i]) - 16)%32 + ord('а'))
        else:
            mes += " "
    mes = mes.replace(' тчк', '.') # Если в сообщении попадетс я точка, она заменется
на тчк
    mes = mes.replace(' зпт', ',') # Если в сообщении попадетс я запятая, она заменется
на зпт
    mes = mes.replace('тире', '-') # Если в сообщении попадетс я - (тире), оно
заменется на тире
    return mes
#print ('Расшифрованное сообщение: ', mes)

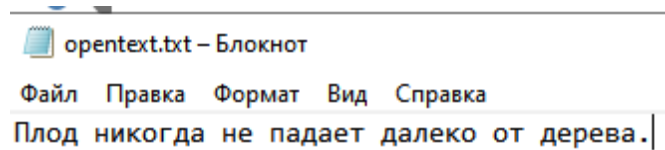
# в этот файл нужно записать исходный текст
f = open(r"opentext.txt", "rt", encoding='utf-8')
mes = f.read()
```

```
# в этот файл записывается зашифрованный текст
f = open('shifr.txt', 'wt', encoding='utf-8')
sh = encryptShannon(str(mes))
f.writelines(sh)
f.close()

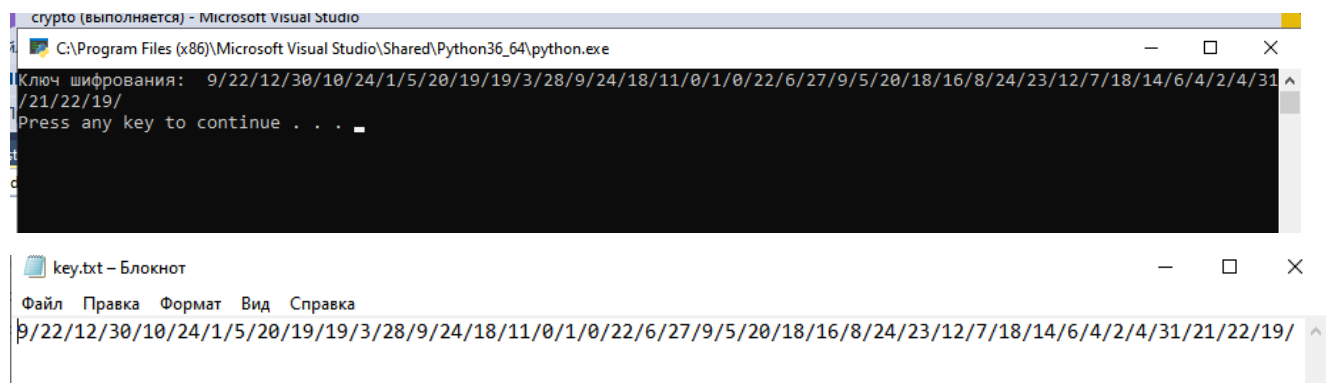
# в этот файл записывается расшифрованный текст
file = open('rasshifr.txt', 'wt', encoding='utf-8')
rassh = decryptShannon(str(sh))
file.writelines(rassh)
file.close()
```

## 5. Тестирование

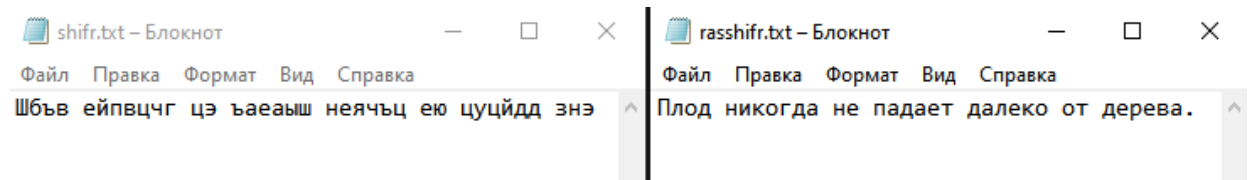
Перед началом работы программы в файл “opentext.txt” записываем исходный текст.



Так выглядит окно выполнения программы. Ключ генерируется программно, а потом, если он понадобится, то его можно найти в файле «key.txt».

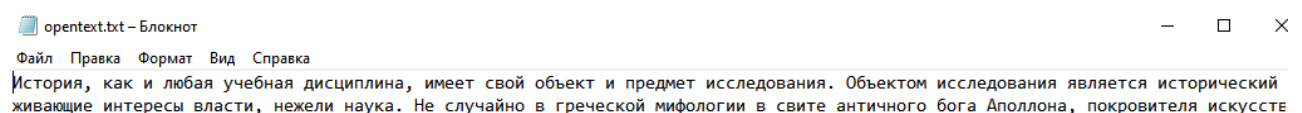


После выполнения программы в файл “shifr.txt” записывается зашифрованный текст, а в файл “rasshifr.txt” расшифрованный текст.



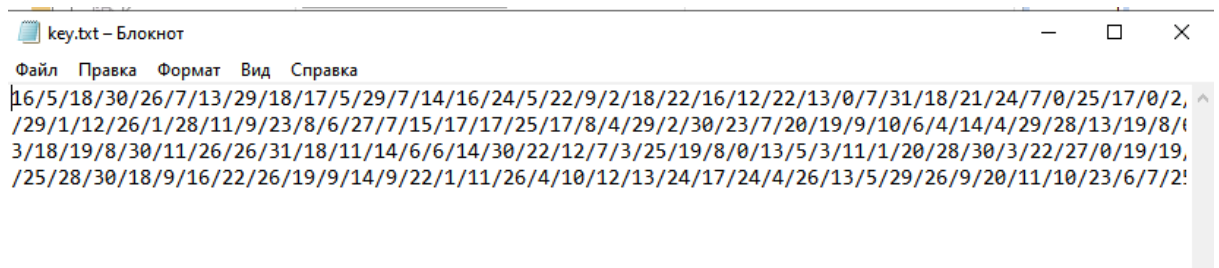
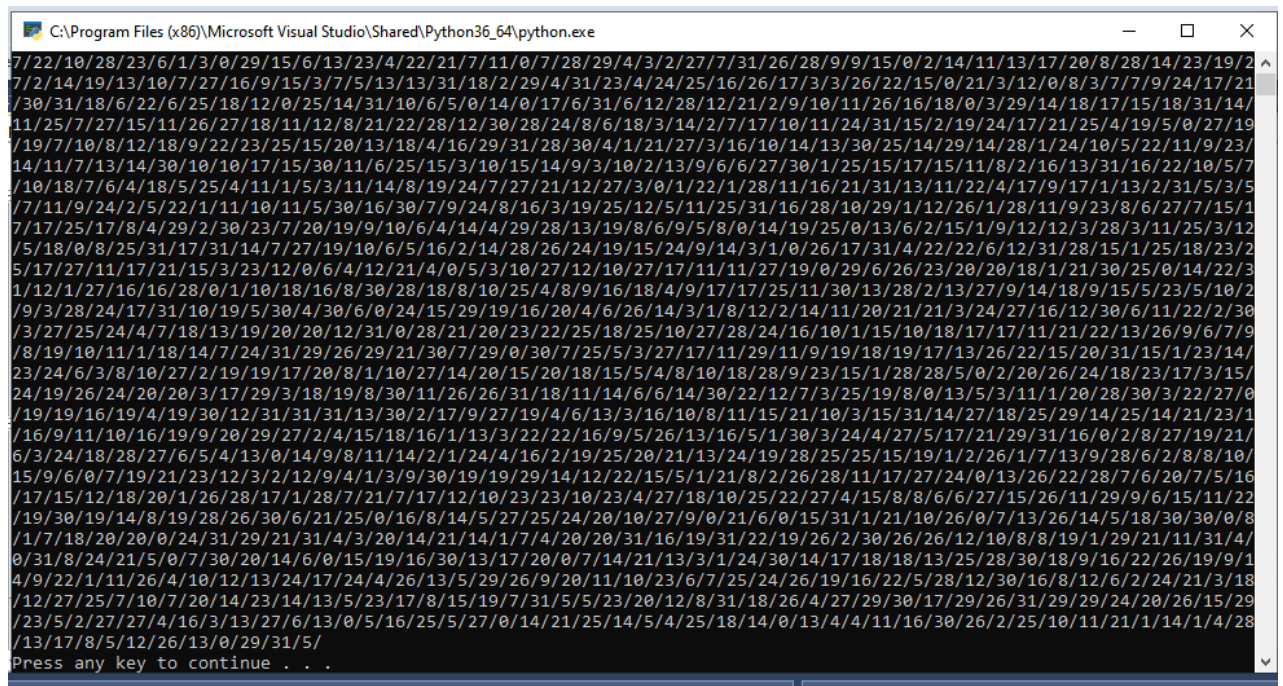
## 6. Работа с текстом не менее 1000 знаков

Перед началом работы программы в файл “opentext.txt” записываем исходный текст. (Полный исходный текст лежит в аннотации)





Так выглядит окно выполнения программы. Ключ генерируется программно, а потом, если он понадобится, то его можно найти в файле «key.txt».

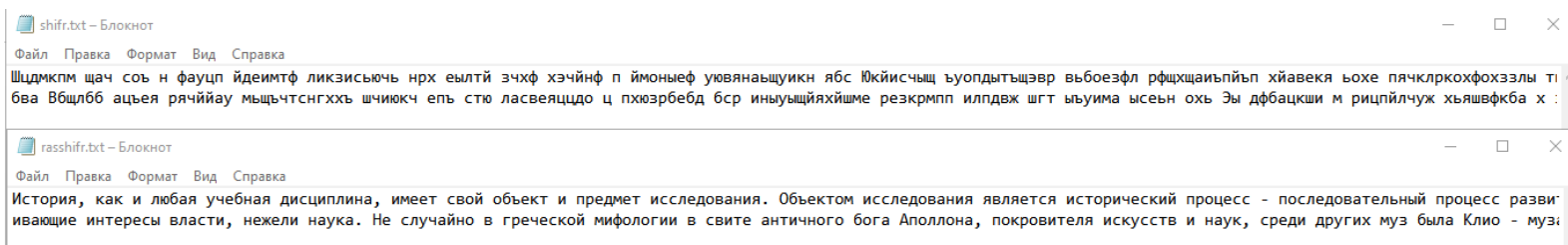


Полный ключ:

16/5/18/30/26/7/13/29/18/17/5/29/7/14/16/24/5/22/9/2/18/22/16/12/22/13/0/7/31/1  
8/21/24/7/0/25/17/0/2/17/22/10/28/23/6/1/3/0/29/15/6/13/23/4/22/21/7/11/0/7/28/2  
9/4/3/2/27/7/31/26/28/9/9/15/0/2/14/11/13/17/20/8/28/14/23/19/27/2/14/19/13/10/7  
/27/16/9/15/3/7/5/13/13/31/18/2/29/4/31/23/4/24/25/16/26/17/3/3/26/22/15/0/21/3/  
12/0/8/3/7/7/9/24/17/21/30/31/18/6/22/6/25/18/12/0/25/14/31/10/6/5/0/14/0/17/6/3  
1/6/12/28/12/21/2/9/10/11/26/16/18/0/3/29/14/18/17/15/18/31/14/11/25/7/27/15/11  
/26/27/18/11/12/8/21/22/28/12/30/28/24/8/6/18/3/14/2/7/17/10/11/24/31/15/2/19/2  
4/17/21/25/4/19/5/0/27/19/19/7/10/8/12/18/9/22/23/25/15/20/13/18/4/16/29/31/28/  
30/4/1/21/27/3/16/10/14/13/30/25/14/29/14/28/1/24/10/5/22/11/9/23/14/11/7/13/14  
/30/10/10/17/15/30/11/6/25/15/3/10/15/14/9/3/10/2/13/9/6/6/27/30/1/25/15/17/15/1  
1/8/2/16/13/31/16/22/10/5/7/10/18/7/6/4/18/5/25/4/11/1/5/3/11/14/8/19/24/7/27/21/  
12/27/3/0/1/22/1/28/11/16/21/31/13/11/22/4/17/9/17/1/13/2/31/5/3/5/7/11/9/24/2/5/  
22/1/11/10/11/5/30/16/30/7/9/24/8/16/3/19/25/12/5/11/25/31/16/28/10/29/1/12/26/  
1/28/11/9/23/8/6/27/7/15/17/17/25/17/8/4/29/2/30/23/7/20/19/9/10/6/4/14/4/29/28/  
13/19/8/6/9/5/8/0/14/19/25/0/13/6/2/15/1/9/12/12/3/28/3/11/25/3/12/5/18/0/8/25/31  
/17/31/14/7/27/19/10/6/5/16/2/14/28/26/24/19/15/24/9/14/3/1/0/26/17/31/4/22/22/6  
/12/31/28/15/1/25/18/23/25/17/27/11/17/21/15/3/23/12/0/6/4/12/21/4/0/5/3/10/27/1

2/10/27/17/11/11/27/19/0/29/6/26/23/20/20/18/1/21/30/25/0/14/22/31/12/1/27/16/1  
6/28/0/1/10/18/16/8/30/28/18/8/10/25/4/8/9/16/18/4/9/17/17/25/11/30/13/28/2/13/2  
7/9/14/18/9/15/5/23/5/10/2/9/3/28/24/17/31/10/19/5/30/4/30/6/0/24/15/29/19/16/20  
/4/6/26/14/3/1/8/12/2/14/11/20/21/21/3/24/27/16/12/30/6/11/22/2/30/3/27/25/24/4/  
7/18/13/19/20/20/12/31/0/28/21/20/23/22/25/18/25/10/27/28/24/16/10/1/15/10/18/  
17/17/11/21/22/13/26/9/6/7/9/8/19/10/11/1/18/14/7/24/31/29/26/29/21/30/7/29/0/3  
0/7/25/5/3/27/17/11/29/11/9/19/18/19/17/13/26/22/15/20/31/15/1/23/14/23/24/6/3/  
8/10/27/2/19/19/17/20/8/1/10/27/14/20/15/20/18/15/5/4/8/10/18/28/9/23/15/1/28/2  
8/5/0/2/20/26/24/18/23/17/3/15/24/19/26/24/20/20/3/17/29/3/18/19/8/30/11/26/26/  
31/18/11/14/6/6/14/30/22/12/7/3/25/19/8/0/13/5/3/11/1/20/28/30/3/22/27/0/19/19/1  
6/19/4/19/30/12/31/31/31/13/30/2/17/9/27/19/4/6/13/3/16/10/8/11/15/21/10/3/15/3  
1/14/27/18/25/29/14/25/14/21/23/1/16/9/11/10/16/19/9/20/29/27/2/4/15/18/16/1/13  
/3/22/22/16/9/5/26/13/16/5/1/30/3/24/4/27/5/17/21/29/31/16/0/2/8/27/19/21/6/3/24/  
18/28/27/6/5/4/13/0/14/9/8/11/14/2/1/24/4/16/2/19/25/20/21/13/24/19/28/25/25/15/  
19/1/2/26/1/7/13/9/28/6/2/8/8/10/15/9/6/0/7/19/21/23/12/3/2/12/9/4/1/3/9/30/19/19  
/29/14/12/22/15/5/1/21/8/2/26/28/11/17/27/24/0/13/26/22/28/7/6/20/7/5/16/17/15/1  
2/18/20/1/26/28/17/1/28/7/21/7/17/12/10/23/23/10/23/4/27/18/10/25/22/27/4/15/8/  
8/6/6/27/15/26/11/29/9/6/15/11/22/19/30/19/14/8/19/28/26/30/6/21/25/0/16/8/14/5/  
27/25/24/20/10/27/9/0/21/6/0/15/31/1/21/10/26/0/7/13/26/14/5/18/30/30/0/8/1/7/18  
/20/20/0/24/31/29/21/31/4/3/20/14/21/14/1/7/4/20/20/31/16/19/31/22/19/26/2/30/2  
6/26/12/10/8/8/19/1/29/21/11/31/4/0/31/8/24/21/5/0/7/30/20/14/6/0/15/19/16/30/13  
/17/20/0/7/14/21/13/3/1/24/30/14/17/18/18/13/25/28/30/18/9/16/22/26/19/9/14/9/2  
2/1/11/26/4/10/12/13/24/17/24/4/26/13/5/29/26/9/20/11/10/23/6/7/25/24/26/19/16/  
22/5/28/12/30/16/8/12/6/2/24/21/3/18/12/27/25/7/10/7/20/14/23/14/13/5/23/17/8/1  
5/19/7/31/5/5/23/20/12/8/31/18/26/4/27/29/30/17/29/26/31/29/29/24/20/26/15/29/2  
3/5/2/27/27/4/16/3/13/27/6/13/0/5/16/25/5/27/0/14/21/25/14/5/4/25/18/14/0/13/4/4/  
11/16/30/26/2/25/10/11/21/1/14/1/4/28/13/17/8/5/12/26/13/0/29/31/5/

После выполнения программы в файл “shifr.txt” записывается  
зашифрованный текст, а в файл “rasshifr.txt” расшифрованный текст.



Полный зашифрованный текст:

Шцдмкпм щач соь н фауцп йдеимтф ликзисьючь нрх еылтй зчхф хэчйнф п  
ймоныеф уювяняьщуикн ябс Юкйисчыщ ъуопдытьцэвр вьбозфл  
рфщхцаиьпйьп хйавека ьохе пчклркохфохззлы тньицаг юлайгбуш  
быфшгъч ж жйячфадз сък жзгэхх хякньсмпя рвыщ эзэрт блачрмк втв р  
изалючц щхдквлврщюн опрбгцвжэфъл хршехю хйипдфючф носдщ ьс Г

рдшйфр нирщрнаамз олимжгй тяз агыййсэ п охсэтцо кципытвкпъжр  
зшющшкэ пзоюзчъжюла ьчщцроцъявлнж крать дчлбццн гье елрннць зыш  
гбуюе л нгцчарцы у фпват ьхньюяву яша тежнз эеш ьобпкт аан  
фгацымрчцох зфх тсхйурвадтяж йлю Ргвзбыд юпзг гпу ьрт итьпймифмяят  
эбы ьбттбсртоб жхшшофну мпщвлцофпач ы ссшкьтйр йээ делийфм ищатсж  
жшх дхгщ ыпотъеис пышжъошт ч ьюушафгвс ошь брмармпдодль хющгшлзс  
жлнлуечгщфнфб ояпнуийб щшскуюнбцдш эдэчвфцхи ь щьтсбнца жсв  
Жбиудшмжа лшрьчарэ влсаыцо наблмхкт дтдхрмрймфич цюрхсббъ двы  
удкхшошн втшр мпоэбует пцйу щ ящцвыбх птм С гичсв бхалшх йпхжфгд  
дндфсфиэюфлх гкьфо юорчтнюэппйцм дзкэнгпйфо збммпй рлш пхкьсп овз  
ыузрьцбефгаыж янфтьк р ощэ япя аьс сщн аяьищтлч пньомвюмвцхяхч т  
дмчинщшижошэои бва Вбщлбб ацьея рячййау мышъчтснгххъ шчиюкч епъ  
стю ласвеяццо ц пхюзрбебд бср иныуыщйяхйшме резкрмпп илпдвж шгт  
ыъуима ысеьн охь Эы дфбацкши м рицпйлчуж хьяшвфкба х зздюг  
ищшкпвсхъ ьхнз Ожыщреюи ьцс феюьцбъмйжъ щодтоокц ч дехе лях мцтдн  
эхогцк ьшл уйлн Оцшм фбър нбид хвьуьвх пцп

Полный расшифрованный текст:

История, как и любая учебная дисциплина, имеет свой объект и предмет исследования. Объектом исследования является исторический процесс - последовательный процесс развития природы и общества, череда сменяющихся друг друга событий, в которых проявляется деятельность многих поколений людей. С каждым мгновением времени, ушедшим в прошлое исторический процесс дополняется совокупностью новых событий, явлений, фактов и факторов в жизни человека, семьи, этноса, государства, человечества. Подобно тому, как материальный мир переживает процессы негэнтропии и энтропии, природа вокруг нас - процессы эволюции и инволюции, человеческое общество характеризуют процессы социального прогресса и регресса. Предметом изучения истории является деятельность главного его субъекта - человека - в прошлом. В узком смысле история представляет собой совокупность социальных фактов, знаний, представлений ученых о том, как эти процессы осуществлялись и осуществляются. Долгое время история существовала скорее, как литература и искусство, обслуживающие интересы власти, нежели наука. Не случайно в греческой мифологии в свите античного бога Аполлона, покровителя искусств и наук, среди других муз была Клио - муза истории.

## 7. Исполняемый файл

Вся работа происходит в файлах: “key.txt”, “opentext.txt”, “shifr.txt”, “rasshifr.txt”.