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 D: Шифры перестановки

Выполнила студентка 3 курса группы 171-341

Решетникова Дарья

Москва 2020 г.

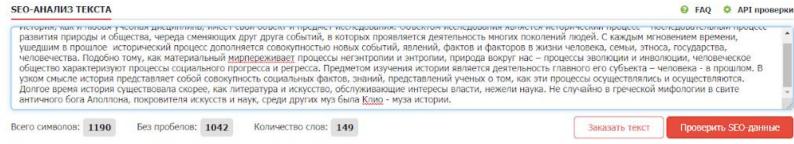
Аннотация

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.



Вертикальная перестановка

1. Описание шифра.

Шифр перестановки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее.

2. Алгоритм шифра.

Можно записать исходное сообщение в прямоугольную матрицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Считывать же шифрованное сообщение по другому маршругу: по вертикали, начиная с правого верхнего угла и двигаясь поочередно сверху вниз и снизу вверх.

Зашифруем, например, таким способом фразу «пример маршрутной перестановки», используя прямоугольник размером 4 х 7 (рис.5.1):

Рис.5.1. Пример шифра маршрутной перестановки		1	2	3	4	5	6	7
	1	П	P	И	М	E	P	M
	2	H	T	У	P	Ш	P	А
	3	0	Й	П	E	P	E	C
	4	И	K	В	0	Н	A	T

Зашифрованная фраза выглядит так:

МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ.

Широко распространена разновидность шифра маршрутной перестановки, называемая шифром вертикальной перестановки. В таком шифре реализуется перестановка считываемых столбцов матрицы в соответствии с ключом. Пусть, например, этот ключ будет таким: 5,4,1,7,2,6,3. Теперь, выбирая столбцы в порядке, заданном ключом, и считывая последовательно буквы каждого из них сверху вниз, следующую криптограмму:

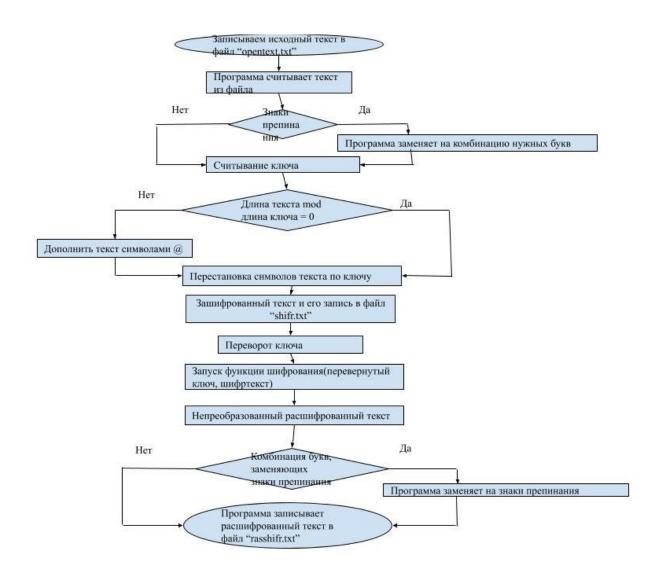
ЕШРНМРЕОПНОИМАСТРТЙКРРЕАИУПВ.

Ключом может быть слово. Например, «ОКТЯБРЬ». Используя расположение букв этого ключа в алфавите, будем иметь набор чисел 3257146 — ключевую последовательность, аналогичную рассмотренной выше, но дающую новый шифртекст:

ЕШРНРТЙКПНОИРРЕАИУПВМАСТМРЕО.

Число ключей шифра вертикальной перестановки, независимо от способа задания, не более m!, где m – число столбцов таблицы шифрования.

3. Блок-схема программы



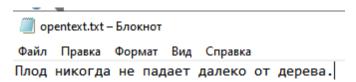
4. Код программы

```
def encryptVertical(text, key):
  text = text.replace('.', ' тчк') # Если в сообщении попадется точка, она
заменется на тчк
  text = text.replace(',', ' зпт') # Если в сообщении попадется запятая, она
заменется на зпт
  text = text.replace('-', 'тире') # Если в сообщении попадется - (тире), оно
заменется на тире
  text = text.replace(' ', 'прбл') #
  n = len(text) #
  m = len(key)
  d = n \% m
  if d != 0:
     for i in range(m - d):
       text += "@"
     n = len(text)
  p = "
  q = 0
```

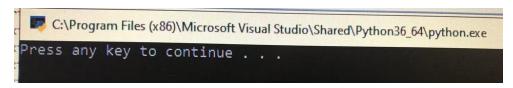
```
while q < n:
    p += ".join(text[q+x] for x in key)
     q += m
  return p
def decryptVertical(text, key):
  # ВТОРНИК
  key = [0, 6, 4, 5, 3, 1, 2]
  dec_key=[]
  for i in range(0,len(key)):
     dec_key.append(key.index(i)) #переворачиваем ключ
  dec_str = encryptVertical(text,dec_key) #используем функцию
шифрования
  dec_str = dec_str.replace('прбл', ' ') # Если в сообщении попадется -
(тире), оно заменется на тире
  dec_str = dec_str.replace(' тчк', '.') # Если в сообщении попадется точка,
она заменется на тчк
  dec_str = dec_str.replace('зпт', ',') # Если в сообщении попадется запятая,
она заменется на зпт
  dec_str = dec_str.replace('тире', '-') # Если в сообщении попадется -
(тире), оно заменется на тире
  dec_str = dec_str.replace('прбл', ") # Если в сообщении попадется - (тире),
оно заменется на тире
  \#l = dec_str.find('.')+1
  \#dec_str = dec_str[:1]
  return dec str
# в этот файл нужно записать исходный текст
key = [0, 6, 4, 5, 3, 1, 2]
f = open(r"opentext.txt", "rt", encoding='utf-8')
text = f.read()
# в этот файл записывается зашифрованный текст
f = open('shifr.txt', 'wt', encoding='utf-8')
sh = encryptVertical(text, key)
f.writelines(sh)
f.close()
# в этот файл записывается расшифрованный текст
file = open('rasshifr.txt', 'wt', encoding='utf-8')
rassh = decryptVertical(sh, key)
file.writelines(rassh)
file.close()
```

5. Тестирование

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



Так выглядит окно выполнения программы.

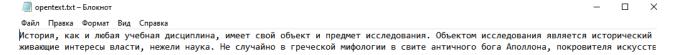


После выполнения программы в файл "shifr.txt" записывается зашифрованный текст, а в файл "rasshifr.txt" расшифрованный текст.

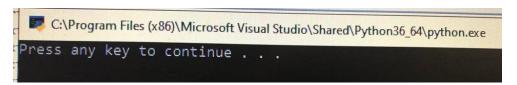


6. Работа с текстом не менее 1000 знаков

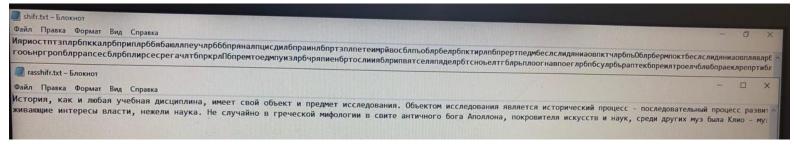
Перед началом работы программы в файл "opentext.txt" записываем исходный текст. (Полный исходный текст лежит в аннотации)



Так выглядит окно выполнения программы. Мы вводим ключ дважды – ключ шифрования и ключ расшифрования соответственно.



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



Полный зашифрованный текст:

Ияриостптзплрбпккалрбприплрббябаюллпеучлрбббпряналпцисдилбпраинлб пртзплпетеимрйвосблпъоблрбелрбпктирлпбпрертпедмбеслслидяниаовпктчлр бпъОблрбермпоктбеслелидяниаовплявлрбяряпсетбртослиийкисчепопрлрбцб прсеслрепртибеслолпдлтеаовьбпрйнылсцеопрсалрбпрзпиятвирррипблолрбпд ыиблобпрщпватесрпптзблреерчблдсблрапмиющяенхрлдбпрудблргпрбпраугл иытбсойплзбпртплвбпррооткблрлрбпыхпявляроебпрятсллтеядеьптьсноргном блипблрхпоиенлкойюллбпрдлрбпейтлрбпчкСалкбпржбпрмдылеовнмгнбпрми елнмеевриплзбпртшлубпрермпидшблрбплвпелошропбпрлрблиортисчпийкес рцропбледрбпссдялноопебпрятслуоквсопютьснопвнодрбысбдрхпопийтбырпп тзблревляблилрбпийзлрбпптфповтакрбприбллртокфаовблрвппзжилрбнчблри пеаеквлоптзплрбпмселрбьзблриппэблртптрапснобртпплзбдсуолгапватрсрппт зблроелчблввстеечачлтбпрколПбпрдропноббпмуолтрпптзблрпаккблреатмблр ыьнлиайилмбпррелпбпрреваиежтрлпбпропсысцерэегнблнипиотрприплрббот рнлэплрбпиизлрбпптпаодррипкволрбрлрбпугнлрбпастбпреирлсцеопрсэблры пвицию олириплрбблвон лию бирицилбирт з плеов лчечи оекесребщоб лсбиротв л такрхаетуюзрипопрлрбцрыпсесбациолслпгооьнргропблррапсесблрбплирсеср егачлтбпркрлПбпремтоедмпуизлрбчряпиенбртослиияблрипвятселяпяделрбтс ноьелтгблрыплоогнавпоеглрбпбсулрбъраптекбпреилтроелчблвбпраеклрепрти блрбплвпмлошропктчлрбпрВплрббмкозлупысмлрбслрбплеияриостпепрлрбдя властесблртпобпрйболуоквсопптьснориоцеблапыхнльртакфблозблрвппзблрт пнрйпианбртпплзбседрлптиенлавйчлубпребпрхнылтблропозблрмппкблртпаэ блркптпблрипрыссеоцпуослрбщявлтеслбпрьислоблрипсвстеущлпсятяюрпчкт блрголДбловблрепрбпряемлиортисяулсбпрщввотесалрбпласпееркорпптзблрп аккблреитлблрпрауатрбприбллсускистлрбпвозлрбпптоиужлбсвпиещаюренти блрбпрыеслиставлитэплрбпжнелрбелрбплинрапкаубркпчлтббпрелНлйчауслн вблроппегрлрбчпойкесроифмбллрипиогблрбплвсрептвибчтинланбпрооглрап гбоблолплАолрбпназлрбпптпиовроктбпряеллсускистиблрвппуналрбкплзбпрт рлсбпрелрбпдидпихгрурпузмблраылбблпиКллрбоилтбпррмблрепулрбпзаиир иостпктчлрбп@@@лрб

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 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.

7. Исполняемый файл

Вся работа происходит в файлах: "opentext.txt", "shifr.txt", "rasshifr.txt".

Решетка Кардано

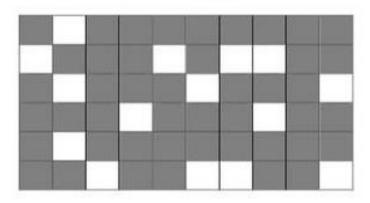
1. Описание шифра.

Поворотные решетки или решетки Кардано по имени придумавшего их Дж.Кардано в XV веке - частный случай шифра маршрутной перестановки.

2. Алгоритм шифра.

используется трафарет из прямоугольного листа клетчатой бумаги размером 2m x 2k клеток. В трафарете вырезано m x k клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.



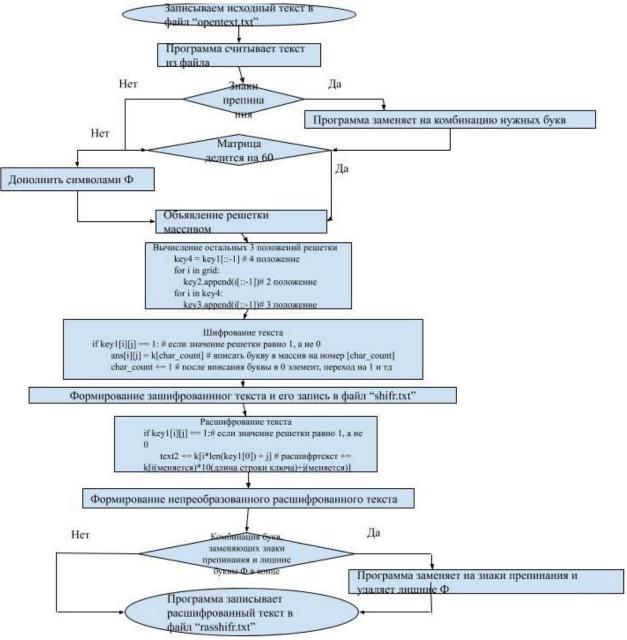
Трафарет шифра «Поворотная решетка».

Число возможных трафаретов (т.е. количество ключей шифра «решетка») составляет

$$T = 4^{m \cdot k}$$

Уже при размерности решетки 8x8 число возможных решеток превосходит 4 миллиарда.

3. Блок-схема программы



4. Код программы

from textwrap import wrap from random import randint

- # Замена некоторых символов на буквенные обозначения def prevr(s):
- s = s.replace('.', 'тк') # Если в сообщении попадется точка, она заменется на тчк
- s = s.replace(',', 'зпт') # Если в сообщении попадется запятая, она заменется на зпт
- s = s.replace('-', 'тире')# Если в сообщении попадется (тире), оно заменется на тире
- s = s.replace(' ', 'прбл') # Если в сообщении попадется пробел, он заменяется на прбл
 - #s = s.replace(' ', ") # Если в сообщении попадется пробел, он удаляется

```
return s
```

```
# в этот файл нужно записать исходный текст
file = open("opentext.txt", "r", encoding='utf-8')#открыть файл для чтения
data = file.read()
file.close()
text = prevr(str(data))
#Если матрица не делится на 60, то заполняем ее буквами Ф
length = len(text)
if len(text) % 60 != 0:
  for i in range(60 - len(text) % 60):
     text += "\phi"
text = wrap(text, 60)
#print(text)
text1 = "
ans = [
  [0, 1, 0, 0, 0, 0, 0, 0, 0, 0]
  [1, 0, 0, 0, 1, 0, 1, 1, 0, 0],
  [0, 1, 0, 0, 0, 1, 0, 0, 0, 1],
  [0, 0, 0, 1, 0, 0, 0, 1, 0, 0],
  [0, 1, 0, 0, 0, 0, 0, 0, 0, 0]
  [0, 0, 1, 0, 0, 1, 1, 0, 0, 1]
     ]
grid = [
  [0, 1, 0, 0, 0, 0, 0, 0, 0, 0],
  [1, 0, 0, 0, 1, 0, 1, 1, 0, 0],
  [0, 1, 0, 0, 0, 1, 0, 0, 0, 1],
  [0, 0, 0, 1, 0, 0, 0, 1, 0, 0],
  [0, 1, 0, 0, 0, 0, 0, 0, 0, 0]
  [0, 0, 1, 0, 0, 1, 1, 0, 0, 1]
     1
key1 = grid #исходное положение решетки - 1
key2 = []
key3 = []
key4 = key1[::-1] # 4 положение
#print("4 положение: ", key4)
for i in grid:
  key2.append(i[::-1])# 2 положение
#print("2 положение: ", key2)
```

```
for i in key4:
  key3.append(i[::-1])# 3 положение
#print("3 положение: ", key3)
#Шифрование текста
char\_count = 0
for k in text:
  for i in range(len(key1)):
     for j in range(len(key1[0])):
       try:
          if key1[i][j] == 1:
             ans[i][j] = k[char\_count]
             char_count += 1
       except:
          pass
  for i in range(len(key2)):
     for j in range(len(key2[0])):
       try:
          if key2[i][j] == 1:
             ans[i][j] = k[char\_count]
             char_count += 1
       except:
          pass
  for i in range(len(key3)):
     for j in range(len(key3[0])):
       try:
          if key3[i][j] == 1:
             ans[i][j] = k[char\_count]
             char_count += 1
       except:
          pass
  for i in range(len(key4)):
     for j in range(len(key4[0])):
       try:
          if key4[i][i] == 1:
             ans[i][j] = k[char\_count]
             char_count += 1
        except:
          pass
  for i in range(len(key2)):
     for j in range(len(key2[0])):
```

```
text1 += ans[i][j]
  char\_count = 0
# в этот файл записывается зашифрованный текст
file = open("shifr.txt", "w", encoding='utf-8')
shifr = text1
file.writelines(shifr)
file.close()
text1 = wrap(text1, 60)
text2 = "
#Расшифрование текста
for k in text1:
  for i in range(len(key1)):
     for j in range(len(key1[0])):
       try:
          if key1[i][j] == 1:
             text2 += k[i*len(key1[0]) + j]
       except:
          pass
  for i in range(len(key2)):
     for j in range(len(key2[0])):
       try:
          if key2[i][j] == 1:
             text2 += k[i*len(key1[0]) + j]
       except:
          pass
  for i in range(len(key3)):
     for j in range(len(key3[0])):
       try:
          if key3[i][j] == 1:
             text2 += k[i*len(key1[0]) + j]
       except:
          pass
  for i in range(len(key4)):
     for j in range(len(key4[0])):
       try:
          if key4[i][j] == 1:
             text2 += k[i*len(key1[0]) + j]
       except:
          pass
```

```
final = "
for k in text2:
  final += k
# в этот файл записывается расшифрованный текст
file = open("rasshifr.txt", "wt+", encoding='utf-8')
#rasshifr = final
final = final.replace('тк','.') # Если в сообщении попадется точка, она
заменется на тчк
final = final.replace('зпт',',') # Если в сообщении попадется запятая, она
заменется на зпт
final = final.replace('тире','-')# Если в сообщении попадется - (тире), оно
заменется на тире
final = final.replace('прбл',' ')# Если в сообщении попадется пробел, он
заменяется на прбл
file.writelines(final[:final.find('\doc')])
file.close()
```

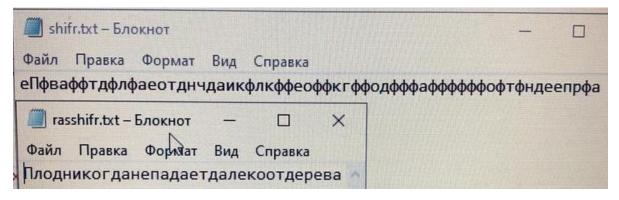
5. Тестирование

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

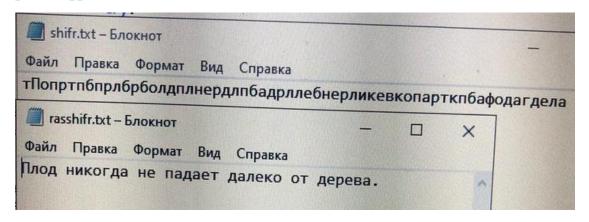
Так выглядит окно выполнения программы.

```
C:\Program Files (x86)\Microsoft Visual Studio\Shared\Python36_64\python.exe
```

После выполнения программы в файл "shifr.txt" записывается зашифрованный текст, а в файл "rasshifr.txt" расшифрованный текст. Так выглядит программа, если пробел заменить на «».



Если пробел заменить на словосочетание «прбл», то текст шифртекст и расшифрованный выглядит так:

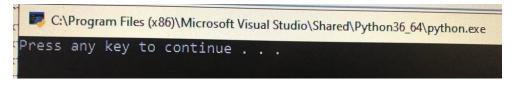


6. Работа с текстом не менее 1000 знаков

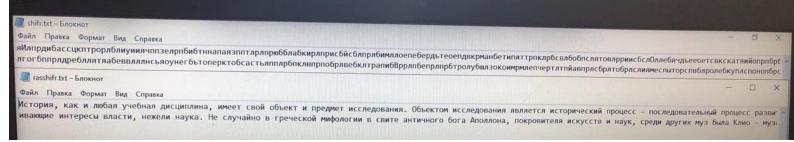
Перед началом работы программы в файл "opentext.txt" записываем исходный текст. (Полный исходный текст лежит в аннотации)



Так выглядит окно выполнения программы. Мы вводим ключ дважды – ключ шифрования и ключ расшифрования соответственно.



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



Полный зашифрованный текст:

яИлпрдибассцкптрорлблиуииячппзелрпбибтннапаязпптлрлпрюбблабкирлпри сбйсблпрлбимллоепебердътеоепдвкрманбетипяттрпклрбсвлбобпслятовлррии сбслОллебячдъееоетсвкскатяийопрпбрбнлилмяппрриблпсьнпрыпбрлрболцей поспресралибзерлвдбиттироицяпоевртатиресербеблиниролщбипориебщррие оехсддитыарвинблррбдлруасзгбитлинмибиолкявоблряытбилдтйзроепурттгыс пахярпппрррббллдбплебвплсрронярийблпнСтпогеильрхпнбрролббслллтюкпь дажпейдтымоккпролблепмлрбушлпебрболвлрмгдемншшеоилнвмоиепезнрпр иблбвлипптсепрмпбррнтуяепнтроосоцреичсссеятпспьркрюбибплйлрбпсолвн одооврпобллкппыпрбрблтлхфпрпбрбфлялаавскклоттебоонывротпрвбприлйб изпйзтипслоемсаьчзвпелпорбивелзткжппаитрззпбпнрлгиблоэсуттпдпрбрблнл лауПозпдлтрповсетвочеабрсзнбтполвтпкапракрблптрбтоклбпрлчбмеампетрб плланмитреррприбебалгллпэпьрненотрыцеоспирсеийжипрвыбапнпрасбипрр избплилтппвбрролббктллрипэуренгппррбрбилтрородлпнпчвоелллорвюцоице юипсцерсичбыиелпзсирпкобтперпрпбрблблэвилоплироалцрьонакбтщееерссо итсгзвыоуоппюпррбрбллспртопобрблхлцаргчеденмриряегерссеесатпспорарм бтбплклрисиблтиорпзрипблрбПулриеблгогбппрлдребллятяабеввлллнсьяоуне гбътоперктобсастьяпплрбпклвпрпобрлвебклтрапибВррлпбепрлпрбтролубшлз окоимрмлепчертлтпйавприсбритобрисяиямеспыторспвбиролебкуписпонопбр средблеоиртлблпрзхеьдпрпбрбнлфласаенткоиатцивоизлеаптнпийврзплптьнп быкрцпресбрсбыблятучломеэпзнтрпыибтхплппросрблупщеррбсблклоаопятбт клвпбрвелолсялрущибмеслясьДптпорврлблбгоиестлпяолютипсррпрттперрва италяапрбпрблублкрлсаасукпкщпрбербллиполррсеетвзиоеббпрлвбрллаблиос клбсуислентустижтезиврптоеспырбвпалзющптирпчнрайечнтеескпжрелоблип кНпроербйпблпрлврбнпрлбмибллфаслукугаооАгопопслллвиотгирепиборплн брбалбозалгптваппррбнбтлпичрбнллбпелндиаипорсккуроуссвкбтизлвтпдпетр рлпугярбилхпбслрпипрбррлрбрблиимбтлклКмлузуиопзфпрафрбпфблрфлббф фылифсффттифлреаппор

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 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.

7. Исполняемый файл

Вся работа происходит в файлах: "opentext.txt", "shifr.txt", "rasshifr.txt".