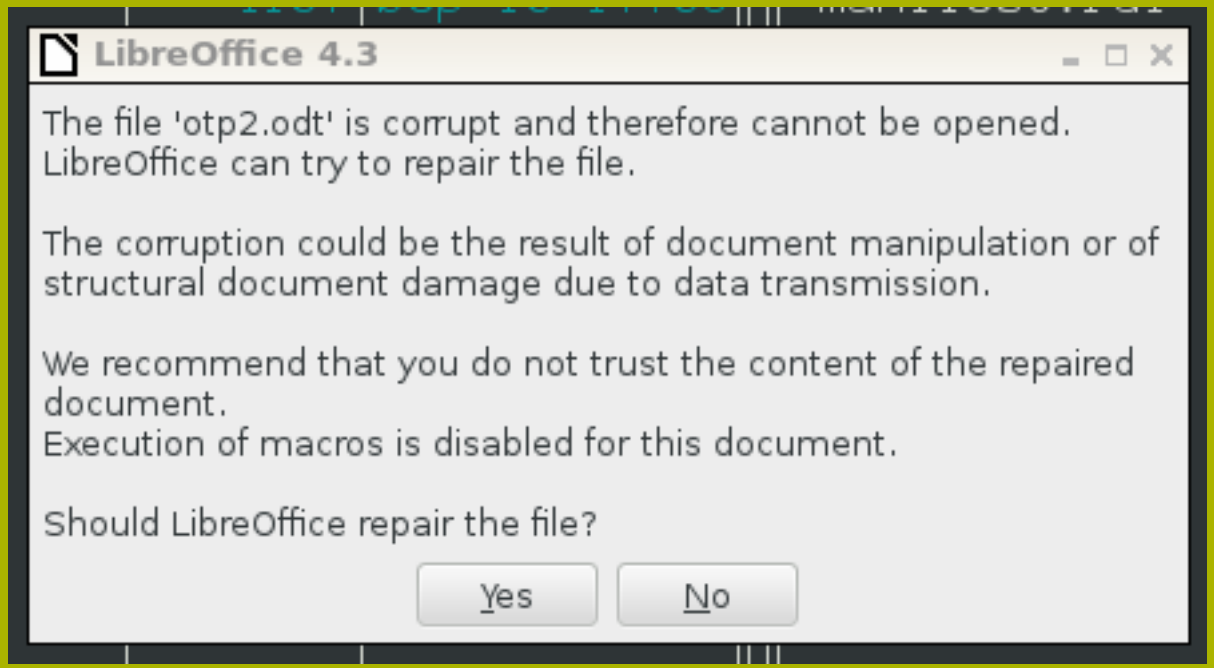
Stegano 300

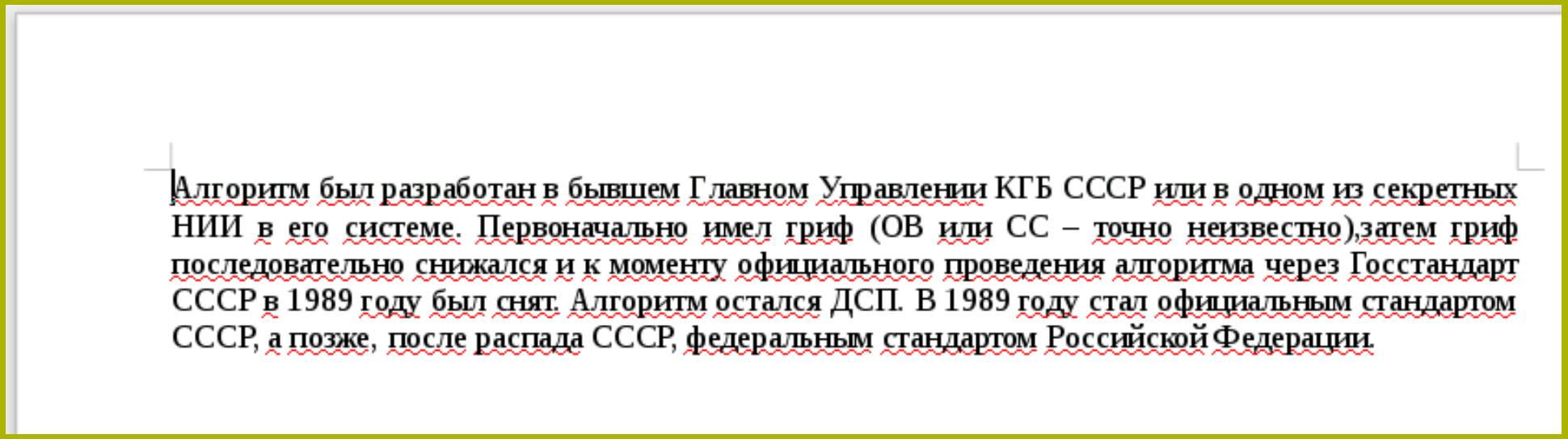
OTP

Задание

В своих старых архивах мы нашли один файл, он испорчен, и не открывается, но один из наших оперативников утверждает, что в нём что-то было... У нас уже давно подозрения по поводу его психического здоровья... Стоит ли ему верить?



Восстановив файл, мы получаем:


Алгоритм был разработан в бывшем Главном Управлении КГБ СССР или в одном из секретных НИИ в его системе. Первоначально имел гриф (ОВ или СС – точно неизвестно),затем гриф последовательно снижался и к моменту официального проведения алгоритма через Госстандарт СССР в 1989 году был снят. Алгоритм остался ДСП. В 1989 году стал официальным стандартом СССР, а позже, после распада СССР, федеральным стандартом Российской Федерации.

Здесь написано что-то про одноразовые блокноты (One time pad)...

Файл имеет формат ODT, значит его можно “разжать” алгоритмом ZIP:

↓n Name	Size	Modify ti
/..	UP--DIR	Sep 13 18
/Configurations2	4096	Sep 13 18
/META-INF	4096	Sep 13 18
/Thumbnails	4096	Sep 13 18
content.xml	6354	Sep 13 10
manifest.rdf	899	Sep 13 10
meta.xml	925	Sep 13 10
mimetype	39	Sep 13 10
settings.xml	10212	Sep 13 10
sstyle	217	Sep 13 17
styles.xml	10086	Sep 13 10

Здесь мы видим какой-то странный файл sstyle, состоящий из 0 и 1

sstyle (~/Documents/computer_...sctf_2015/Rainbow/r1/otp2) - VIM

```
  1 0100111000011101111100100001100111010111101100111011011011110000101110000
    1111110101000100011001001001101111011011100101111111111111000011110100101
    0100001001111110010011100011100101010001111101111100101010110110101000010
~
~
~
~
<rity_6/for_krasctf_2015/Rainbow/r1/otp2/sstyle" 1L, 217C 1,1          All
```

Декодировать его не удастся, поэтому оставим его (наверное, это и есть блокнот).

Если открыть файл content из архива ODT

```
−<office:body>
 −<office:text>
  −<text:sequence-decls>
     <text:sequence-decl text:display-outline-level="0" text:name="Illustration"/>
     <text:sequence-decl text:display-outline-level="0" text:name="Table"/>
     <text:sequence-decl text:display-outline-level="0" text:name="Text"/>
     <text:sequence-decl text:display-outline-level="0" text:name="Drawing"/>
   </text:sequence-decls>
  −<text:p text:style-name="p0">
     <text:span text:style-name="t1">Ал</text:span>
     <text:span text:style-name="t8">г</text:span>
     <text:span text:style-name="t7">о</text:span>
     <text:span text:style-name="t3">р</text:span>
     <text:span text:style-name="t4">и</text:span>
     <text:span text:style-name="t5">т</text:span>
     <text:span text:style-name="t4">м б</text:span>
     <text:span text:style-name="t2">ы</text:span>
     <text:span text:style-name="t8">л р</text:span>
     <text:span text:style-name="t1">а</text:span>
     <text:span text:style-name="t8">з</text:span>
     <text:span text:style-name="t7">ра</text:span>
     <text:span text:style-name="t3">б</text:span>
```

Почему почти все буквы оформляются разными стилями?

Заглянем в файл со стилями и увидим, что стили задают цвет текста с небольшим отклонением от черного в компоненте Green (max на 3 бита).

```
styles = {
    '#000100': "000",
    '#000200': "001",
    '#000300': "010",
    '#000400': "011",
    '#000500': "100",
    '#000600': "101",
    '#000700': "110",
    '#000800': "111",
    }
```

Если теперь каждому цвету сопоставить 3-битовую последовательность и записать их в последовательности соответствующих букв текста, получим бинарную строку, которая, к слову тоже не может быть декодирована.

```
000111110010011100011001111000111110010000100110011000010111101000

Process finished with exit code 0
```

Теперь воспоминаем про одноразовые блокноты и складываем две бинарные строки (можно было обратить внимание на одну длину) по модулю 2.

```
In [1]: s1 = "01100000011111001001110001101101100111111111100011111011001000010011001100001011110100000001001000101011101101111111011010011000110000011000000000011000101011110011011010000100001100000110001101111101110000111100101011"

In [2]: s2 = "00100111000011101111100100001100111010111101100111011011011110000101110000111100100010000110010010011011101101110010111111111111100001111010010100001001111110010011100011100101010000111110111110010101011011010100001"

In [3]: len(s1)
Out[3]: 216

In [4]: len(s2)
Out[4]: 216

In [5]: "".join([str(int(s1[i],2) ^ int(s2[i],2)) for i in range(len(s1))])
Out[5]: '010001110111001001100101011000010111010000100001001000000101100101101111011101010111001000100000011001100110110001100001011001110010000001101001011100110010000000100011001100010011000100110001001100010011000100110010'
```

И получаем флаг:

```
Great! Your flag is #111112

Process finished with exit code 0
```