Отчет по лабораторной работе №8

Информационная безопасность

Паландузян АК НПИбд-01-18

Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

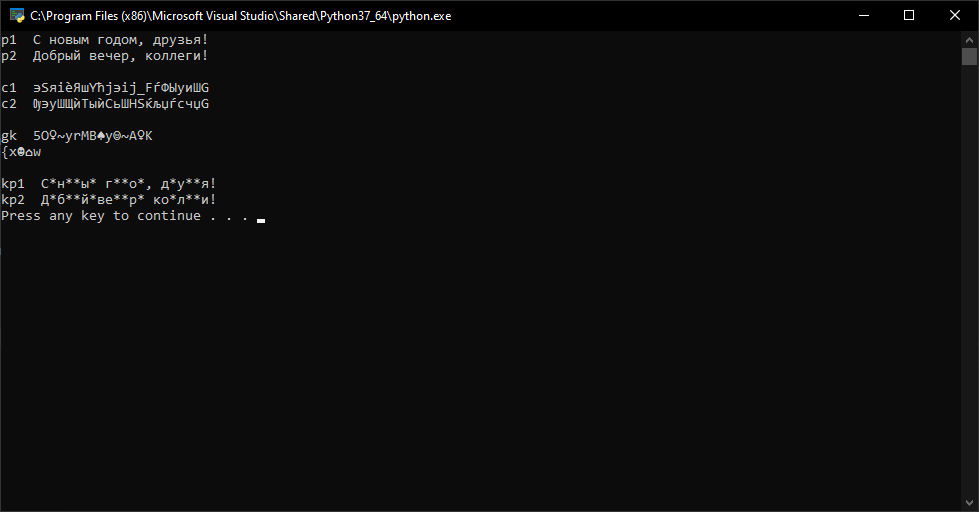
# Выполнение лабораторной работы

1. Модернизируем код, написанный в предыдущей лабораторной работе:

p1 = 'С новым годом, друзья!'  
p2 = 'Добрый вечер, коллеги!'  
k = 'lsrhbdtyhfyhdsfgdhttgf'  
c1 = ''  
c2 = ''  
  
print('p1 ', p1)  
print('p2 ', p2, '\n')  
  
c1 = ''  
c1 = c1.join(chr(ord(i) ^ ord(j)) for i, j in zip(p1, k))  
print('c1 ', c1)  
c2 = ''  
c2 = c2.join(chr(ord(i) ^ ord(j)) for i, j in zip(p2, k))  
print('c2 ', c2, '\n')  
  
kp1 = 'С\*н\*\*ы\* г\*\*о\*, д\*у\*\*я!'  
kp2 = ''  
gk = ''  
  
gk = gk.join(chr(ord(i) ^ ord(j)) for i, j in zip(c1, c2))  
print('gk ', gk, '\n')  
  
kp2 = kp2.join('\*' if i == '\*' else chr(ord(i) ^ ord(j)) for i, j in zip(kp1, gk))  
print('kp1 ', kp1)  
print('kp2 ', kp2)

В переменных P запишем текст, в k - ключ, а в C - шифротекст. kp1 - Известная часть первого текста kp2 - Известная часть второго текста. Пока что она пустая, но в дальнейшем часть символов станет известна. gk - ключ, получаемый при гаммировании двух шифротекстов, что равно гаммированию двух текстов.

1. Злоумышленнику известно kp1, c1 и c2. Для получения части kp2 злоумышленник гаммирует c1 и c2, получает gk. Затем он гаммирует kp1 по ключу gk, получает kp2. Часть символом из 1 и 2 текста всё ещё неизвестно, однако у злоумышленника есть возможность методом подстановки подобрать символы так, чтобы при гаммировании смысл обоих текстов не терялся. Таким образом можно сузить круг поиска, в некоторых случаях даже отыскать точные значения p1 и p2.
2. Вывод программы:



Вывод

# Контрольные вопросы

1. Как, зная один из текстов ( или ), определить другой, не зная при этом ключа?
2. Что будет при повторном использовании ключа при шифровании текста?  
   Текст будет расшифрован.
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?  
   По формулам режима однократного гаммирования:
4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

* Ключ даст возможность расшифровать оба текста
* С помощью открытого текста можно расшифровать другие известные шифротексты
* Часть текста можно узнать, используя заранее известный шаблон и формат другого текста

1. Перечислите преимущества шифрования одним ключом двух открытых текстов.

* Скорость шифрования
* Простота алгоритма
* Большие изменения шифротекста в случае изменения ключа или открытого текста

# Выводы

На основе проделанной работы освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.