

Отчет по лабораторной работе №8

Информационная безопасность

Паландузян АК НПИбд-01-18

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Контрольные вопросы	8
4	Выводы	10

List of Figures

2.1 ВЫВОД 7

1 Цель работы

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

2 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  = ''

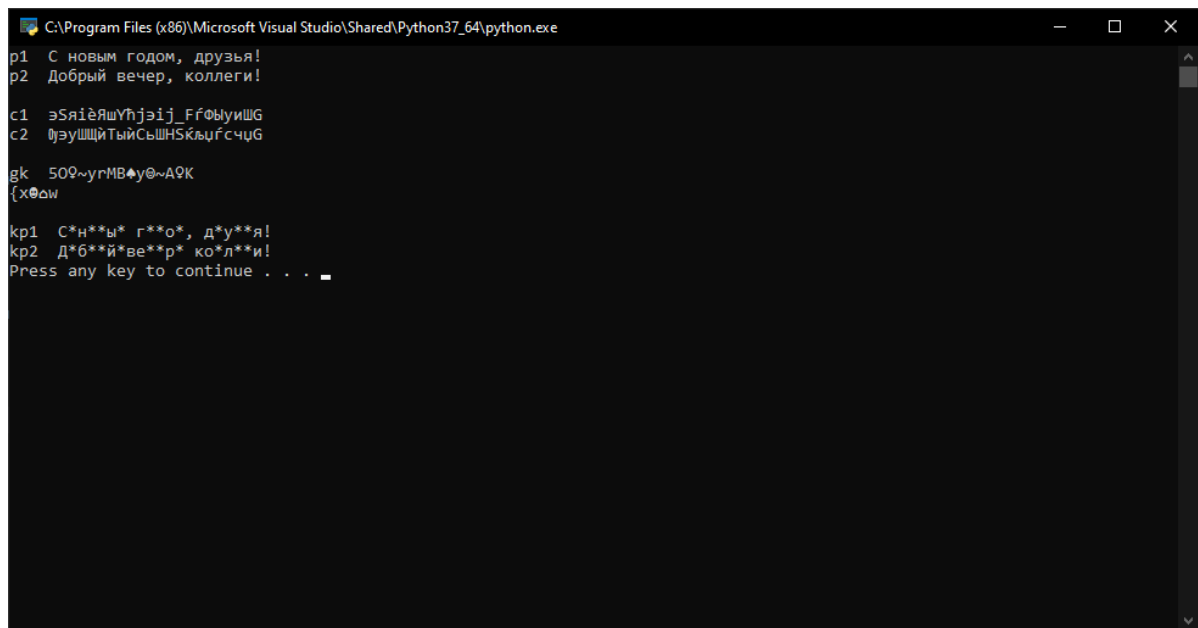
gk = gk.join(chr(ord(i) ^ ord(j)) for i, j in zip(c1, c2))
```

```
print('gk ', gk, '\n')
```

```
kp2 = kp2.join('*' if i == '*' else chr(ord(i) ^ ord(j)) for i, j in zip(  
print('kp1 ', kp1)  
print('kp2 ', kp2)
```

В переменных Р запишем текст, в k - ключ, а в С - 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.

2. 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.
3. Вывод программы:



```
C:\Program Files (x86)\Microsoft Visual Studio\Shared\Python37_64\python.exe
p1 С новым годом, друзья!
p2 Добрый вечер, коллеги!
c1 эSяіёяшYнјэіј_ҒғФыиШG
c2 0эуШЩйТййСьШНСкьѳсцG
gk 509~yгMB▲y@~A9K
{x00w
kp1 С*н**ы* г**о*, д*у**я!
kp2 Д*б**й*ве**р* ко*л**и!
Press any key to continue . . .
```

Figure 2.1: Вывод

3 Контрольные вопросы

1. Как, зная один из текстов (P_1 или P_2), определить другой, не зная при этом ключа?

$$C_1 \oplus C_2 \oplus P_1 = P_1 \oplus P_2 \oplus P_1 = P_2$$

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:

$$C_1 = P_1 \oplus K_1$$

$$C_2 = P_2 \oplus K_2$$

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

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

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

4 Выводы

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