Отчет по лабораторной работе №7

Информационная безопасность

Паландузян АК НПИбд-01-18

Содержание

List of Figures

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Выполнение лабораторной работы

Разработаем приложение с возможность гаммирования на Python:

```
text = 'С новым годом, друзья!'
key = 'Добрый вечер, коллеги!'

res1 = ''
res1 = res1.join(chr(ord(i) ^ ord(j)) for i, j in zip(text, key))
print(res1)

res2 = ''
res2 = res2.join(chr(ord(i) ^ ord(j)) for i, j in zip(key, res1))
print(res2)
```

1. В начале объявим переменные ключа и текста
2. Затем применим алгоритм гаммирования и запишем результат в res1. Выводим его. Это шифротекст.
3. Таким же образом, но с переменной res2, гаммируем шифротекст с ключом, чтобы получить текст.
4. Аналогично можно выполнить гаммирование текста по шифторексту, в этом случае получим ключ.
5. Вывод программы:

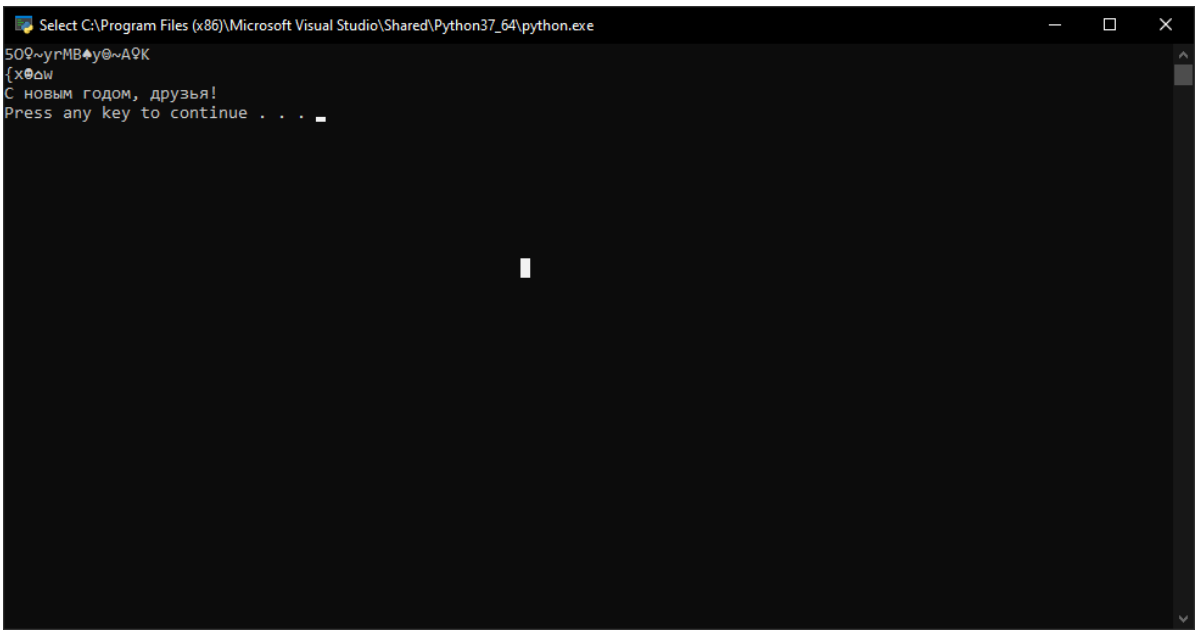

Figure 2.1: Вывод

3 Контрольные вопросы

1. Поясните смысл однократного гаммирования. Каждый символ текста и ключа попарно побитово складываются по XOR.
2. Перечислите недостатки однократного гаммирования. Ключ нельзя использовать повторно, при этом также имеется ограничение по символам, ведь размер ключа должен быть равен размеру текста.
3. Перечислите преимущества однократного гаммирования. Симметричность алгоритма и криптостойкость.
4. Почему длина открытого текста должна совпадать с длиной ключа? Каждый символ текста должен попарно складываться с символом ключа, а это невозможно в случае, если количество символов разное — будут символы, к которым нет пары.
5. Какая операция используется в режиме однократного гаммирования, назовите её особенности? Сложение по модулю 2 (XOR): при сложении чисел с другим получается исходное. Если в методе шифрования используется однократная вероятностная гамма той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть.
6. Как по открытому тексту и ключу получить шифротекст? Сложить попарно символы текста с ключом по модулю 2.
7. Как по открытому тексту и шифротексту получить ключ? Сложить попарно по модулю 2 символы открытого текста с символами шифротекста.

8. В чём заключаются необходимые и достаточные условия абсолютной стойкости шифра?

- Полная случайность ключа
- Равенство длин ключа и открытого текста
- Использование ключа однократно

4 Выводы

Освоил на практике применение режима однократного гаммирования.