Отчёт по лабораторной работе 7

Простейший вариант

Еленга Невлора Люглеш

Содержание

# 1 Цель работы

Освоить на практике применение режима одно кратного гаммирования .

# 2 Алтуальность

Шифрование в режиме однократного гаммирования – это один из методов симметричного шифрования, который используется для защиты информации от несанкционированного доступа.

# 3 Выполнение лабораторной работы

1.Определили вид шифро текст а при известном ключе и известном открытом тексте.

* Код

import numpy as np   
  
 def gen\_key(text):  
 rn = np.random.randint(0, 255, len(text))  
 key = [hex(e)[2:] for e in rn]  
  
 return key  
  
 def Crypt(open\_text, key):  
 print(f"Open Text: {open\_text}")  
 hex\_open\_text = []  
 for ch in open\_text:  
 hex\_open\_text.append(ch.encode("cp1251").hex())  
  
 print("Hex Open Text: ", \*hex\_open\_text)  
  
   
 print("Key: ", \*key)  
 hex\_crypted\_text = []  
 for i in range(len(hex\_open\_text)):  
 hex\_crypted\_text.append("{:02x}".format(int(key[i], 16)^int(hex\_open\_text[i], 16)))  
  
 print("Hex Crypted Text: ", \*hex\_crypted\_text)  
 crypted\_text = bytearray.fromhex("".join(hex\_crypted\_text)).decode("cp1251")  
 print(f"Crypted Text:{crypted\_text}")  
  
 return crypted\_text

* Результаты

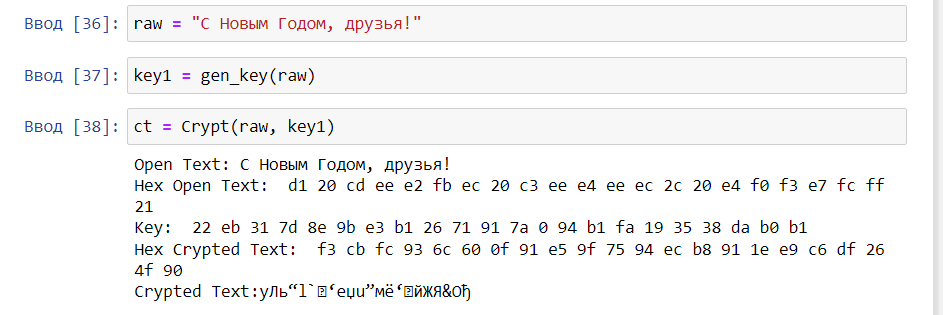


Рис. 1.1.Шифрование Текста в режиме однократного гаммирования

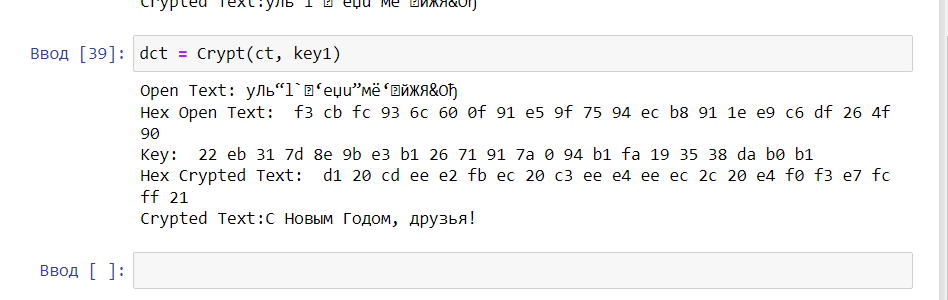


Рис. 1.2.Дешифрование Текста

2.Определили ключ,спомощью которого шифро текст может быть преобразован в некоторый фрагмент текста,представляющий собой один из возможных вариантов прочтения открытого текста.

def find\_key(open\_text, crypted\_text):  
 print(f"Open Text: {open\_text}\nCrypted Text: {crypted\_text}")  
 hex\_open\_text = []  
 for ch in open\_text:  
 hex\_open\_text.append(ch.encode("cp1251").hex())  
  
 hex\_crypted\_text = []  
 for ch in crypted\_text:  
 hex\_crypted\_text.append(ch.encode("cp1251").hex())  
  
 print("Hex Open Text: ", \*hex\_open\_text)  
 print("Hex Crypted Text: ", \*hex\_crypted\_text)  
 key = [hex(int(i,16)^int(j,16))[2:] for (i,j) in zip(hex\_open\_text, hex\_crypted\_text)]  
 print("key ", \*key)  
  
 return key

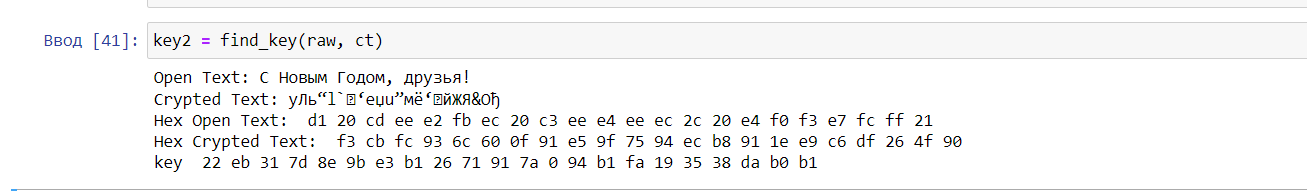


Рис. 1.3.

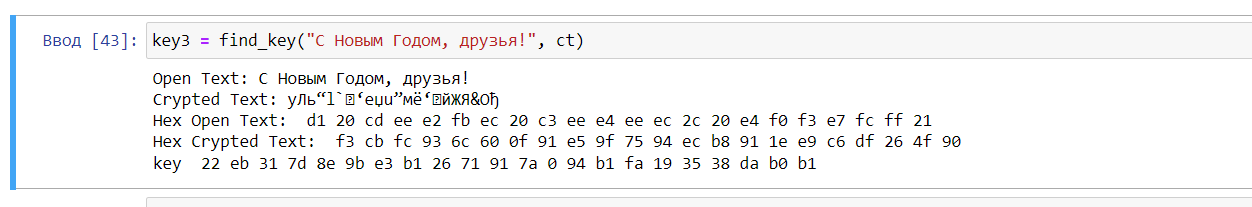


Рис. 1.4.Дешифрование Текста

## 3.1 Контрольные вопросы

1.Поясните смысл одно кратного гаммирования.

С точки зрения теории криптоанализа метод шифрования однократной случайной равновероятной гаммой той же длины (“однократное гаммирование”), что и открытый текст, является невскрываемым. Обоснование, которое привел Шеннон, основываясь на введенном им же понятии информации, не дает возможности усомниться в этом - из-за равных априорных вероятностей криптоаналитик не может сказать о дешифровке, верна она или нет. Кроме того, даже раскрыв часть сообщения, дешифровщик не сможет поправить положение - информация о вскрытом участке гаммы не дает информации об остальных ее частях.

2.Недостатки одно кратного гаммирования.

Первый недостаток данного метода – это необходимость использования случайного ключа-гаммы для каждого сообщения. Если ключ-гамма повторяется или становится известен злоумышленнику, то метод становится небезопасным. Также, генерация сложных случайных последовательностей может привести к высоким требованиям к вычислительной мощности компьютера, что может создать сложности в процессе шифрования больших объемов данных.

Второй недостаток – это отсутствие защиты от целенаправленной атаки. При использовании шифрования в режиме однократного гаммирования злоумышленник может применить метод анализа частотности, при котором исследуется частота повторений определенных битов в шифротексте. Это может привести к открытию ключа-гаммы и расшифровке сообщения.

3.Преимущества одно кратного гаммирования.

Высокий уровень безопасности: Шифрование методом гаммирования с использованием случайной гаммы обеспечивает высокий уровень безопасности. При правильной реализации и использовании достаточно длинной и случайной гаммы, расшифровка сообщения без знания гаммы становится практически невозможной; Отсутствие паттернов; Высокая скорость шифрования и расшифрования.

6.Для того, чтобы получить зашифрованный текст достаточно сложить каждый символ открытого текста с символом гаммы. В качестве гаммы будет выступать символьная последовательность произвольной длины. В случае, если ее длина меньше длины текста, мы просто повторим последовательность нужное количество раз, чтобы хватило на зашифровку всего текста.

Расшифровка выполняется аналогичным образом. Складываем символы зашифрованного текста с символами гаммы и получаем открытый текст.

8.Необходимые и достаточные условия абсолютной стойкости шифра:

· полная случайность ключа;

· равенство длин ключа и открытого текста;

· однократное использование ключа.

# 4 Вывод

В ходе выполнения лабораторной работы мы освоили на практике применение режима одно кратного гаммирования.