#### Лабораторная работа

Номер 4

Прокопьева М. Е.

Российский университет дружбы народов, Москва, Россия

## Информация

#### Докладчик

- Прокопьева Марина Евг.
- студент
- Бизнес-инфороматика
- Российский университет дружбы народов

#### Вводная часть

Цель работы



Освоить на практике применение режима однократного гаммирования

# Порядок выполнения работы

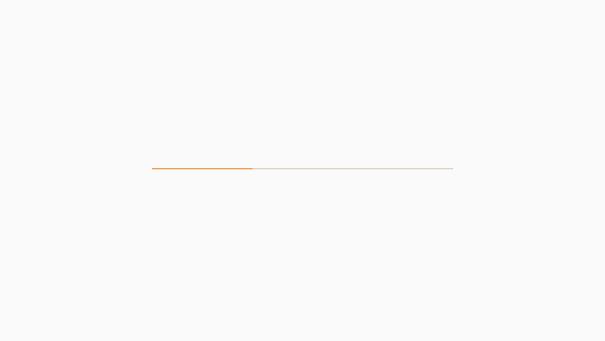
#### Порядок выполнения работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: 1. Определить вид шифротекста при известном ключе и известном откры- том тексте. 2. Определить ключ, с помощью которого шифротекст может быть преоб- разован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста

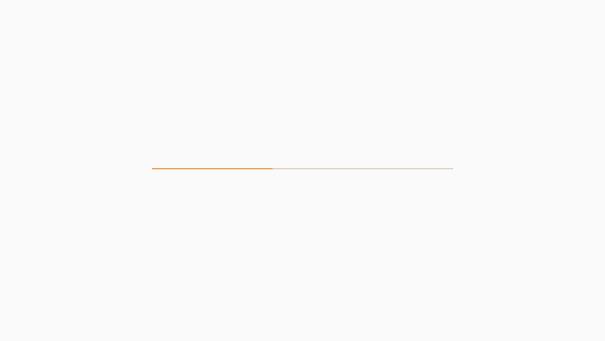
#### Теоретическое введение

#### Теоретическое введение

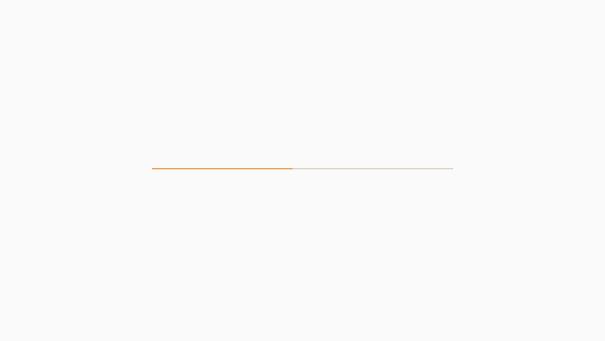
Предложенная Г. С. Вернамом так называемая «схема однократного использования (гаммирования)» (рис. 7.1) является простой, но надёжной схемой шифрования данных. Гаммирование представляет собой наложение (снятие) на открытые (за- шифрованные) данные последовательности элементов других данных, по-лученной с помощью некоторого криптографического алгоритма, для по-лучения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого пред- ставляет собой известную часть алгоритма шифрования.



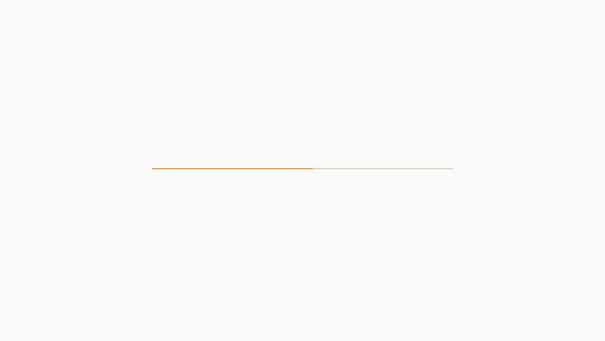
В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком 🗋) между элементами гаммы и элементами подлежащего сокрытию текста. Напомним, как рабо- тает операция XOR над битами:  $0 \square 0 = 0, 0 \square 1 = 1, 1$  $\Box 0 = 1, 1 \Box 1 = 0$ . Такой метод шифрования является симметричным, так как двойное при- бавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же про-граммой.



Если известны ключ и открытый текст, то задача нахождения шифротек- ста заключается в применении к каждому символу открытого текста следу- ющего правила: Ci = Pi  $\square$  Ki, (7.1) где Ci — i-й символ получившегося зашифрованного послания, Pi - i-й символ открытого текста, Ki - i-й символ ключа, i = 1, m. Размерности открытого текста и ключа должны совпадать, и полученный шифротекст будет такой же длины. Если известны шифротекст и открытый текст, то задача нахождения ключа решается также в соответствии с (7.1), а именно, обе части равен- ства необходимо сложить по модулю 2 с Рі: Сі □ Рі = Рі  $\square$  Ki  $\square$  Pi = Ki, Ki = Ci  $\square$  Pi.



Открытый текст имеет символьный вид, а ключ — шестнадцатеричное представление. Ключ также можно представить в символьном виде, воспользовавшись таблицей ASCII-кодов. К. Шеннон доказал абсолютную стойкость шифра в случае, когда одно- кратно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения. Криптоалгоритм не даёт никакой ин- формации об открытом тексте: при известном зашифрованном сообщении С все различные ключевые последовательности К возможны и равноверо- ятны, а значит, возможны и любые сообщения Р. Необходимые и достаточные условия абсолютной стойкости шифра: – полная случайность ключа; – равенство длин ключа и открытого текста; - однократное использование ключа.



Рассмотрим пример. Ключ Центра: 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54 Сообщение Центра: Штирлиц — Вы Герой!! D8 F2 E8 F0 EB E8 F6 20 2D 20 C2 FB 20 C3 E5 F0 EE E9 21 21 Зашифрованный текст, находящийся у Мюллера: DD FE FF 8F E5 A6 C1 F2 B9 30 CB D5 02 94 1A 38 E5 5B 51 75 Дешифровальщики попробовали ключ: 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 55 F4 D3 07 BB BC 54 и получили текст: D8 F2 E8 F0 EB E8 F6 20 2D 20 C2 FB 20 C1 EE EB E2 E0 ED 21 Штирлиц - Вы Болван!

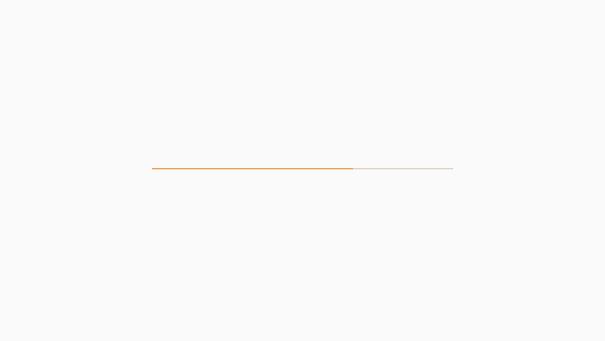
Другие ключи дадут лишь новые фразы, пословицы, стихотворные строфы, словом, всевозможные тексты заданной длины.

Выполнение лабораторной

работы

#### Выполнение лабораторной работы

Я выполнала лабораторную работа на языке программирования Python, листинг программы и результаты выполнения приведены в отчете.



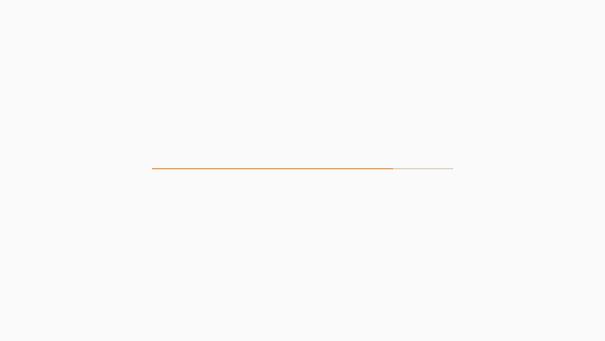
```
import random
import string
def generate key hex(text):
    key = ''
    for i in range(len(text)):
        key += random.choice(string.ascii letters + string.digits)
    return kev
def en_de_crypt(text, key):
    new text = ''
    for i in range(len(text)):
        new text += chr(ord(text[i]) ^ ord(kev[i % len(kev)]))
    return new text
```

## Ответы на контрольные

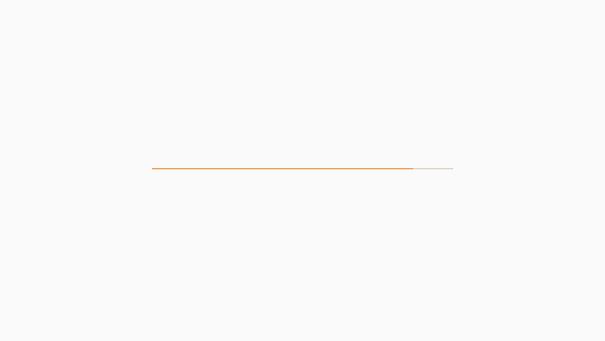
вопросы

#### Ответы на контрольные вопросы

- 1. Поясните смысл однократного гаммирования. Однократное гаммирование это метод шифрования, при котором каждый символ открытого текста гаммируется с соответствующим символом ключа только один раз.
- 2. Перечислите недостатки однократного гаммирования. Недостатки однократного гаммирования:
  - Уязвимость к частотному анализу из-за сохранения частоты символов открытого текста в шифротексте.
  - Необходимость использования одноразового ключа, который должен быть длиннее самого открытого текста.
  - Нет возможности использовать один ключ для шифрования разных сообщений.



- 3. Перечислите преимущества однократного гаммирования. Преимущества однократного гаммирования:
  - Высокая стойкость при правильном использовании случайного ключа.
  - Простота реализации алгоритма.
  - Возможность использования случайного ключа.
- 4. Почему длина открытого текста должна совпадать с длиной ключа? Длина открытого текста должна совпадать с длиной ключа, чтобы каждый символ открытого текста гаммировался с соответствующим символом ключа.



- 5. Какая операция используется в режиме однократного гаммирования, назовите её особенности? В режиме однократного гаммирования используется операция ХОК (исключающее ИЛИ), которая объединяет двоичные значения символов открытого текста и ключа для получения шифротекста. Особенность ХОК если один из битов равен 1, то результат будет 1, иначе 0.
- 6. Как по открытому тексту и ключу получить шифротекст? Для получения шифротекста по открытому тексту и ключу каждый символ открытого текста гаммируется с соответствующим символом ключа с помощью операции XOR.
- 7. Как по открытому тексту и шифротексту получить ключ? По открытому тексту и шифротексту невозможно восстановить действительный ключ, так как для этого нужна информация о каждом символе ключа.

14/15

8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра - Необходимые и достаточные условия абсолютной

### Выводы



Освоила на практике применение режима однократного гаммирования.