Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Кекишева А.Д.

16 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Кекишева Анастасия Дмитриевна
- Бизнес-информатика
- Кафедра теории веротности и кибербезопасности
- Российский университет дружбы народов
- 1032201194@pfur.ru
- https://github.com/adkekisheva

Цель работы

Цель работы

Освоить на практике применение режима однократного гаммирования.

Задание

Задание

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 открытом тексте. 2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Выполнение лабораторной работы

Шаг 1

Шаг 1

```
def main(de_text, en_text):   # de - расшифрованный, en - зашифрованный
    dict = {"а": 1, "б": 2, "в": 3, "г": 4, "д": 5, "е": 6, "ё": 7, "ж": 8, "з": 9,
            "и": 10, "й": 11, "к": 12, "л": 13, "м": 14, "н": 15,"о": 16, "п": 17,
            "р": 18, "с": 19, "т": 20, "у": 21, "ф": 22, "х": 23, "ц": 24, "ч": 25,
            "ш": 26, "щ": 27, "ъ": 28, "ы": 29, "ь": 30, "э": 31, "ю": 32, "я": 33,
            " ": 34, ",": 35, "!": 36}
    dict2 = {n: m for m, n in dict.items()}
    digits_de_text = list()
    digits_en_text = list()

    for i in de_text:
        digits_de_text.append(dict[i])
    print("Числа текста: ", digits_de_text)

    for j in en_text:
        digits_en_text.append(dict[j])
    print("Числа зашифрованного текста: ", digits_en_text)

    digits_res = list()
    h = 0

    for i in de_text:
        try:
            a = dict[i] + digits_en_text[h]
        except:
            h = 0
            a = dict[i] + digits_en_text[h]
        if a >= 36:
            a = a % 36
        h += 1
        digits_res.append(a)
    print("Числа шифровки: ", digits_res)
```

Шаг 2

```
text_en = ""
for i in digits_de_text:
    text_en += dict2[i]
print("Шифровка: ", text_en)

digits = list()
for i in text_en:
    digits.append(dict[i])
h = 0
digits1 = list()
for i in digits:
    a = i - digits_en_text[h]
    if a < 1:
        a = 36 + a
    digits1.append(a)
    h += 1
text_de = ""

for i in digits1:
    text_de += dict2[i]
print("Рассшифровка: ", text_de)
```

Рис. 2: Вторая часть алгоритма

Шаг 3

Шаг 3

```
text = "С Новым Годом, друзья!"
de_text = text.lower()
print(de_text)
```

```
с новым годом, друзья!
```

```
len(de_text)
```

```
22
```

```
en_text = "шнта оамтмтанл прщуты!"
len(en_text)
```

```
22
```

```
main(de_text, en_text)
```

```
Числа текста:  [19, 34, 15, 16, 3, 29, 14, 34, 4, 16, 5, 16, 14, 35, 34, 5, 18, 21, 9, 30, 33, 36]
Числа зашифрованного текста:  [26, 15, 20, 1, 34, 16, 1, 14, 20, 14, 20, 1, 15, 13, 34, 17, 18, 27, 21, 20, 29, 36]
Числа шифровки:  [9, 13, 35, 17, 1, 9, 15, 12, 24, 30, 25, 17, 29, 12, 32, 22, 0, 12, 30, 14, 26, 0]
Шифровка:  с новым годом, друзья!
Рассшифровка:  ысэндллттбун,ф!ц!ьциг!
```

Рис. 3: Результат

Выводы

Выводы

Освоила на практике применение режима однократного гаммирования, написав программу, которая определяет вид шифротекста при известном ключе и известном открытом тексте и определяет ключ.