Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Абу Сувейлим Мухаммед Мунифович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Освоить на практике применение режима однократного гаммирования [1].

2 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.

3 Выполнение лабораторной работы

Во-первых, нужно импортировать нужные библиотеки командой:

```
import os
```

Далее, для максимально эффективной работы лучше выполнять команды на уровне битов. Для этого мы напиши функцию xor_bytes наложения гаммы:

```
def xor_bytes(text, key):
    return bytes([a ^ b for a, b in zip(text, key)])
```

Далее, напишем две функции для encoding и decoding:

```
def encrypt(text):
    text_bytes  = text.encode('utf-8') # Converet text to bytes
    key = os.urandom(len(text_bytes))
    cipherText = xor_bytes(text_bytes, key)
    return cipherText, key


def decrypt(cipherText, key):
    org_text_bytes = xor_bytes(cipherText, key)
    return org_text_bytes.decode('utf-8')
```

Выполняем пример из учебника:

```
text = "С Новым Годом, друзья!"
cipherText, key =  encrypt(text)
```

```
print(f"Cipher text: {cipherText}")
print(f"Key: {key}")
decryptText = decrypt(cipherText, key)
print(f"Decrypted text: {decryptText}")
```

Получаем такой результат:

```
Cipher text: b'\x1a<]\x0cc\x81\x00\xf5B{"{\xb1\xc3\xf1\x1e\x82\x94RUOZ\xee^\xf2K*ua\xf
Key: b'\xca\x9d}\xdc\xfeQ\xbe%\xf0\xaa\xa9\xab\r\xe3!\x8dR*\x82\xe1\x9f\xe4>\xe2\xdek\
Decrypted text: С Новым Годом, друзья!
```

Если в Key поминать значения на другие, например на:

```
key1 = b'\xca\x9d}\xdc\xfeQ\xbe%\xf0\xaa\xa9\xab\r\xe3!\x8dR*\x82\xe1\x9f\xe4>\xe2\xde
decryptText = decrypt(cipherText, key1)
print(f"Decrypted text: {decryptText}")
```

получим:

```
Decrypted text: С Новым Годом, зIузья!
```

4 Выводы

Основали на практике применение режима однократного гаммирования.

Список литературы

1. Kulyabov D., Korolkova A., Gevorkyan M. Информационная безопасность компьютерных сетей: лабораторные работы. 2015.