Лабораторная работа №7

Ramzi A. Al-Dorikhim

RUDN University, 2022 Moscow, Russia

Цель выполнения лабораторной работы

Освоить на практике применение режима однократного гаммирования.

Результат работы шифровательа

```
[4] k, t, et = encryption(s)

    Открытый текст:  С Новым Годом, друзья!

    Открытый текст в 16-ой системе:  ['d1', '20', 'cd', 'ee', 'e2', 'fb', 'ec', '20', 'c3', 'ee', 'e4', 'ee', 'ec', '2c', '20', 'e4', 'f0', 'f3', 'e7', 'fc', 'ff', '21']

    Ключ в 16-ой системе:  ['91', 'ea', 'ba', 'ef', 'e', '43', '94', '46', '44', '6', '9a', '93', '34', '5b', '90', '34', '4d', '9c', '6d', 'b5', 'e5', 'bb']

    Шифротекст в 16-ой системе:  ['40', 'ca', '77', '01', 'ec', 'b8', '78', '66', '87', 'e8', '7e', '7d', 'd8', '77', 'b0', 'd0', 'bd', '6f', '8a', '49', '1a', '9a']

    Шифротекст:  @Kw▯mёxf‡и~}Шw°PSoЊI▯ь
```

Результат работы дешифрователя

```
key = find_key(s, et)

Открытый текст:  С Новым Годом, друзья!

Шифротекст:  @KwBмёxf‡и~}ШwºPSoЬIBь

Открытый текст в 16-ой системе:  ['d1', '20', 'cd', 'ee', 'e2', 'fb', 'ec', '20', 'c3', 'ee', 'e4', 'ee', 'ec', '2c', '20', 'e4', 'f0', 'f3', 'e7', 'fc', 'ff', '21']

Шифротекст текст в 16-ой системе:  ['40', 'ca', '77', '01', 'ec', 'b8', '78', '66', '87', 'e8', '7e', '7d', 'd8', '77', 'b0', 'd0', 'bd', '6f', '8a', '49', '1a', '9a']

Найденный ключ в 16-ой системе:  ['91', 'ea', 'ba', 'ef', 'e', '43', '94', '46', '44', '6', '9a', '93', '34', '5b', '90', '34', '4d', '9c', '6d', 'b5', 'e5', 'bb']
```

Вывод

В ходе данной лабораторной работы я освоила на практике применение режима однократного гаммирования.

Спасибо за внимание