

Лабораторная работа № 7. Элементы криптографии.

Однократное гаммирование

Ндри Ив Алла Ролан

2023 Sep 12th

Цель работы

Освоить на практике применение режима однократного гаммирования

Результат выполнения лабораторной работы



```
+ Code + Text
def crypt_string(open_text):
    print(f"open text: {open_text}")
    hex_open_text = []
    for ch in open_text:
        hex_open_text.append(ch.encode("cp1251").hex())

    print(f"Hex Open Text: ", *hex_open_text)
    key = np.random.randint(0, 255, len(open_text))
    hex_key = [hex(e)[2:] for e in key]

    print(f"Hex key: ", *hex_key)
    hex_crypted_text = []
    for i in range(len(hex_open_text)):
        hex_crypted_text.append("{}{:02x}".format(int(hex_key[i], 16)^int(hex_open_text[i], 16)))

    print(f"Hex Crypted Text: ", *hex_crypted_text)
    crypted_text = bytearray.fromhex("".join(hex_crypted_text).decode("cp1251"))
    print(f"Crypted Text: {crypted_text}")

    return key, hex_crypted_text, crypted_text

key1, hct, ct = crypt_string("С Новым Годом, друзья!")

open text: С Новым Годом, друзья!
Hex Open Text: d1 20 cd ee e2 fb ec 20 c3 ee e4 ee ec 2c 20 e4 f0 f3 e7 fc ff 21
Hex key: 9 90 18 9f d9 3b 1f 25 2f ed b5 80 7d 5d a8 36 38 37 42 26 2a ed
```

Рис. 1: 1

в данной работе мы освоили практическое применение одиночного гамма-режима