

Лабораторная работа №8

Уваров Илья НПИбд-02-19

Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Выполнение лабораторной работы

1. Написал код на языке python, позволяющий шифровать и дешифровать данные в режиме однократного гаммирования.(рис. 1).

```
def create_key(size=6, chars=str.ascii_lowercase):
    for _ in range(size):
        def hexadecimal_form(s): return ' '.join("%02x" % ord(i) for i in s)
        def gamming(fst_text, sec_text):
            fst_text_ascii = [ord(i) for i in fst_text]
            sec_text_ascii = [ord(i) for i in sec_text]
            for s, k in zip(fst_text_ascii, sec_text_ascii):
                P1, P2 = "ПримерТекста1", "ПримерДругогоТекста2"
            print('Исходные тексты:')
            print(P1) print(P2) key=create_key(len(P1))
            print("для кодирования текстов:", create_key)
            print("Шестнадцатичный ключ для кодирования:", hexadecimal_form(key))
            print("для открытого текста 1 и ключа:", hexadecimal_form(fst_text_ascii))
            print("Шифротекст для открытого текста 2 и ключа:", hexadecimal_form(sec_text_ascii))
            print("тексты путём гаммирования двух шифротекстов:")
            print(gamming(gamming(P1, key)+gamming(P2, key)))
            print(gamming(gamming(P1, key)+gamming(P2, key)))
```

Исходные тексты:
ПримерТекста1
ПримерДругогоТекста

Ключ для кодирования текстов: 3Uugw4iH5z8aA
Шестнадцатиричный ключ для кодирования текстов: 36 41 35 32

Шифротекст для открытого текста 1 и ключа: ЩЁЙЎӨиѡіЪЧЈψи
Шифротекст для открытого текста 2 и ключа: ЩЁЙЎӨиЎУKsVӨ○

Получим тексты путём гаммирования двух шифровок и исходного
6A52GxJcYfJAD
6A52Gx| 6Вы470

Выводы

Освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.