Лабораторная 8

Болотина А.С.

Цель работы

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

Задание

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Листинг

```
import random as rnd
import string as str

#Пишем небоходимые функции

def create_key(size=10, chars=str.ascii_letters + str.digits):
    return ''.join(rnd.choice(chars) for _ in range(size))


def hexadical_form(s):
    return ''.join("{:02x}".format(ord(c)) for c 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]
    return ''.join(chr(s^k) for s,k in zip(fst_text_ascii,sec_text_ascii))

#Выполним шифрование
P1, P2 = 'example', 'hello world'
print(f'original texts: {P1}, {P2}')
key=create_key(len(P1))

print('Key for encoding:', create_key(len(P1)))
print('Hexadecimal key for encoding:', hexadical_form(key))
print('Ciphertext for plaintext 1 and the key:', gamming(P1, key))
print('Ciphertext for plaintext 2 and the key:', gamming(P2, key))
print('The result of the gamming of two ciphers and the source text:')
print(gamming(gamming(P1, key)+gamming(P2, key), P1))
print(gamming(gamming(P1, key)+gamming(P2, key), P2))
```

Результат выполнения

```
original texts: example, hello world
Key for encoding: 5DBNmdn
Hexadecimal key for encoding: 584f5335794e77
Ciphertext for plaintext 1 and the key: =72X    "
Ciphertext for plaintext 2 and the key: 0*?Yn
The result of the gamming of two ciphers and the source text:
XOS5yNw
UR^4fe_XS=
```

Выводы

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