Лабораторная работа № 8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Миленин Иван Витальевич

Цель работы

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

ХОД РАБОТЫ

Блок функций для дальнейшего криптоанализа

```python
import random
import string

def generate_new_key(size=6, chars = string.ascii_letters + string.digits):
    return ''.join(random.choice(chars) for _ in range(size))
def hexadecimal_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))
```

Блок обработки данных и вывода требуемых значений

```
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"
print("Исходные тексты:\n", "P1: ", P1, "\nP2: ", P2, sep='')
key = generate_new_key(len(P1))
print("Ключ для кодирования обоих текстов:")
print(key)
print("В шестнадцатиричном виде:")
print(hexadecimal_form(key))

C1 = gamming(P1, key)
C2 = gamming(P2, key)

print("\nШифротекст C1 для открытого текста P1 и ключа key")
print(C1, "--- C1")
print("Шифротекст C2 для открытого текста P2 и ключа key")
print(C2, "--- C2")

crypto_sum = gamming(C1, C2)

print("\nПолучим первый текст путем гаммирования двух шифровок и второго текста:")
print("Вычисленный P1:", gamming(crypto_sum, P2))
print("Получим второй текст путем гаммирования двух шифровок и первого текста:")
print("Вычисленный P2:", gamming(crypto_sum, P1))
```

Вывод значений и результат работы

```
Исходные тексты:
P1: НаВашисходящийот1204
P2: ВСеверныйфилиалБанка
Ключ для кодирования обоих текстов:
PUr989yaBY3TasPykjM6
В шестнадцатиричном виде:
50 55 72 39 38 39 79 61 42 59 33 54 61 73 50 79 6b 6a 4d 36

Шифротекст C1 для открытого текста P1 и ключа key
эѥѠЉѰЁиФѼѫѼНљъѮлZX}? --- C1
Шифротекст C2 для открытого текста P2 и ключа key
тVчЋЙѹфЪѺНЋѮљужѪћїѶI --- C2

Получим первый текст путем гаммирования двух шифровок и второго текста:
Вычисленный P1: НаВашисходящийот1204
Получим второй текст путем гаммирования двух шифровок и первого текста:
Вычисленный P2: ВСеверныйфилиалБанка
```

Аналитическое обоснование дешифровки

$$1 \oplus 1 = 0, \quad 1 \oplus 0 = 1$$

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

$$C_1 \oplus C_2 \oplus P_1 = P_1 \oplus P_2 \oplus P_1 = P_2$$

Вывод

В ходе работы мы успешно на практике освоили применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.