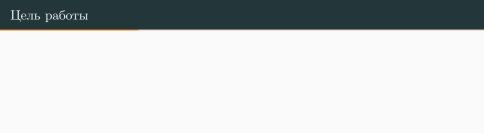
Лабораторная работа № 8

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

Абакумов Егор Александрович



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

Ход работы

Блок функций для дальнейшего криптоанализа

```
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))
```

```
1 P1 = "НаВашисходящийот1204"
2 Р2 = "ВСеверныйфилиалБанка"
3 print("Исходные тексты:\n", "P1: ", P1, "\nP2: ", P2, sep='')
4 key = generate new key(len(P1))
5 print("Ключ для кодирования обоих текстов:")
6 print(key)
7 print("В шестнадцатиричном виде:")
8 print(hexadecimal form(key))
10 C1 = gamming(P1, key)
11 C2 = gamming(P2, key)
13 print("\nШифротекст С1 для открытого текста Р1 и ключа kev")
14 print(C1, "--- C1")
15 print("Шифротекст С2 для открытого текста Р2 и ключа key")
16 print(C2, "--- C2")
18 crypto sum = gamming(C1, C2)
20 print("\nПолучим первый текст путем гаммирования двух шифровок и второго текста:")
21 print("Вычисленный Р1:", gamming(crypto sum, P2))
22 print("Получим второй текст путем гаммирования двух шифровок и первого текста:")
23 print("Вычисленный Р2:", gamming(crypto_sum, P1))
```

Вывод значений и результат работы

```
Исходные тексты:
Р1: НаВашисходящийот1204
Р2: ВСеверныйфилиалБанка
Ключ для кодирования обоих текстов:
РUг989уаВУЗТаяРукјМ6
В шестнадцатиричном виде:
50 55 72 39 38 39 79 61 42 59 33 54 61 73 50 79 6b 6a 4d 36

Шифротекст С1 для открытого текста Р1 и ключа key
энсМиЧЕйОйойонь₃ЭлХУ№ --- С1
Шифротекст С2 для открытого текста Р2 и ключа key
ТVчБИуфьонБъъужыйТVI --- С2

Получим первый текст путем гаммирования двух шифровок и второго текста:
Вычисленный Р1: НаВашисходящийот1204
Получим Творой текст путем гаммирования двух шифровок и первого текста:
Вычисленный Р2: 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.