Лабораторная работы №7

Павлова В.Ю.

Цель работы

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

Ход работы

Задаю данные, перевожу их в байты и задаю ключ. (рис. [-@fig:001])

```
C1 = xor_encrypt_decrypt(P1_bytes, K)
C2 = xor_encrypt_decrypt(P2_bytes, K)
print("Шифротекст C1: ", C1.hex())
print("Шифротекст C2: ", C2.hex())
```

```
Шифротекст C1:  d591c7cfdedce7624598d996f3d62e4ddb0ca0e0d483c6f6def6e76b44aed8ac1365cffc
Шифротекст C2:  d59ec7dedefbe76044a5d8aef2ea2e43db0ba1d0d5b4c7c4def6e76244abd9bff2e72f75db08a0e4
```

данные

Ход работы

Пишу функцию для шифрования(рис. [-@fig:002])

```
P1_xor_P2 = bytes([c1 ^ c2 for c1,c2 in zip(C1, C2)])
```

```
P2_recovered = bytes([p1 ^ p1_p2 for p1, p1_p2 in zip(P1_bytes, P1_xor_P2)])
print("Восстановленный текст P2: ", P2_recovered.decode('utf-8'))
```

```
Восстановленный текст P2:  ВСеверныйфилиалБан
```

функция

Ход работы

Шифрование P1 и P2. (рис. [-@fig:003])

```
P1 = "НаВашисходящийот1204"
P2 = "ВСеверныйфилиалБанка"
P1_bytes = P1.encode('utf-8')
P2_bytes = P2.encode('utf-8')
K = bytes.fromhex("050C177F0E4E37D29410092E2257FFC80BB27054")
```

шифрование

Ход работы

Находим P2, зная C1, C2 и P1 (рис. [-@fig:004])

```
def xor_encrypt_decrypt(text_bytes, key_bytes):
    return bytes([b^key_bytes[i % len(key_bytes)] for i,b in enumerate(text_bytes)])
```

P2

Вывод

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.