

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего
образования «Самарский национальный исследовательский университет имени академика
С. П. Королева»
(Самарский университет)

Институт информатики и кибернетики

Кафедра информационных систем и технологий

ОТЧЁТ

по лабораторной работе №2
по курсу «Защита информации»

Вариант 2

Выполнил,
обучающийся группы № 6304-090301D_____ И. И. Алеев

Проверил,
доцент кафедры ИСТ_____ В.В. Графкин

Самара 2023

Дата проведения лабораторной работы: 20.02.2023г

Задание

Задание 1. Дешифровать слово, зашифрованное шифром Цезаря

Задание 2. Дешифровать слово, зашифрованное шифром Вернама с 2-битовым ключом.

Задание 3. Дешифровать фразу, зашифрованную методом простой замены.

Задание 4. Рассчитать бит четности для указанного набора данных.

Задание 5. Рассчитать CRC-3 для указанных данных и порождающего полинома.

Задание 6. Восстановить число, защищенное продольно-поперечным контролем четности. Порядок нумерации битов числа и синдрома:

7654		5
0123		4
<hr/>		
3210		

Задание 7. Восстановить число, защищенное кодом Хэмминга.

Задание 1

Программа:

```
enc_word = "ДЁЕПОЙИН".lower()
alph = "АВВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ".lower()
base = ord(alph[0])

for i in range
    (len(alph)): for ch in
enc_word:
    print(alph[(ord(ch) - base + i) % len(alph)],
end='') print(f"+ {i}")
```

Результат:

```
шхщгвэьб+ 20
щцъдгюэв+ 21
ъчыедяюг+ 22
ышьжеаяд+ 23
ьщээжбае+ 24
...
азблкдей+ 28
бювмлжек+ 29
вягнмэжл+ 30
гадонизм+ 31
```

Задание 2

Программа:

```
code = [ (b | b << 2 | b << 4 | b << 6) for b in
range(4)]print([bin(i) for i in code])

data =
b'\xd1\xd0\xc3\xdd\xd9\xd5\xc3\xdd\xca'buf
= []

for c in code:
    for ch in data:
        buf.append(ch ^
c)
    print(bytes(buf).decode('cp866'))
    buf = []
```

Результат:

```
... ['\x0b', '\x0b1010101', '\x0b1010101', '\x0b1111111']
тллл
ДЕЦИМАЦИЯ
{ziws iw`
./<"&*<"5
```

Задание 3 –

Пропущено

Задание 4

Программа:

```
data = 87
par =
False
for i in range(32):
    par ^= True if (data << i) & 1 == 1 else

Falseprint(f"{bin(data)}\t{par}")
```

Результат:

```
| ... 0b1010111      True
```

Задание 5

Программа:

```
d = 59
pol = 4
n = 3

def crc(d: int, dl: int) ->
    int: if ( d < pol):
        return d
    print(f"{bin(d)}\n{bin(pol << dl)}\n{bin(d ^ (pol <<
dl))}\n") return crc(d ^ (pol << dl), dl-1)

print(crc(59, 3))
```

Результат:

```
... 0b111011
    0b100000
    0b11011

    0b11011
    0b10000
    0b1011

    0b1011
    0b1000
    0b11

    3
```

Задание 6

Решение:

Handwritten solution on grid paper:

111 = 0110 1111 29 = 01 1101

Binary addition (XOR):

$$\begin{array}{r} 0110 \mid 00 \\ 1111 \mid 01 \\ \hline 1001 \\ 1101 \\ \oplus 001001 \\ 01 \end{array}$$

Result:

$$\Rightarrow 0110 1101 = 109$$

Результат:

1 бит искажён, оригинальные данные 109

Задание 7

Решение:

data: 2 8 = 011 1100

syn: 4

3, 4, 5 = 011, 100, 101

6. syn: $011 \oplus 100 \oplus 101 = 010 = 2$

$4 \oplus 2 = 100 \oplus 010 = 110 = 6$

\Rightarrow 6 бит искажён.

проверка

011 11100

3, 4, 5, 6 = 011, 100, 101, 110

$011 \oplus 100 \oplus 101 \oplus 110 = 100 = 4$

коды совпадают

Результат:

искажён 6 бит, оригинальные данные 60