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

Выпонлил,	
обучающийся группы № 6304-090301D	И. И. Алеев
Проверил,	
доцент кафедры ИСТ	В.В. Графкин

Дата проведения лабороторной 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:

Задание 7. Восстановить число, защищенное кодом Хэмминга.

Задание 1

Программа:

```
enc_word = "ДЁЕПОЙИН".lower()

alph = "АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ".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:

```
шхщгвэь6+ 20
щцъдгюэв+ 21
ъчыедяюг+ 22
ышьжеаяд+ 23
ьщэзжбае+ 24
...
аэблкедй+ 28
бювмлжек+ 29
вягнмзжл+ 30
гадонизм+ 31
```

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 = []</pre>
```

Результат:

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}")</pre>
```

Результат:

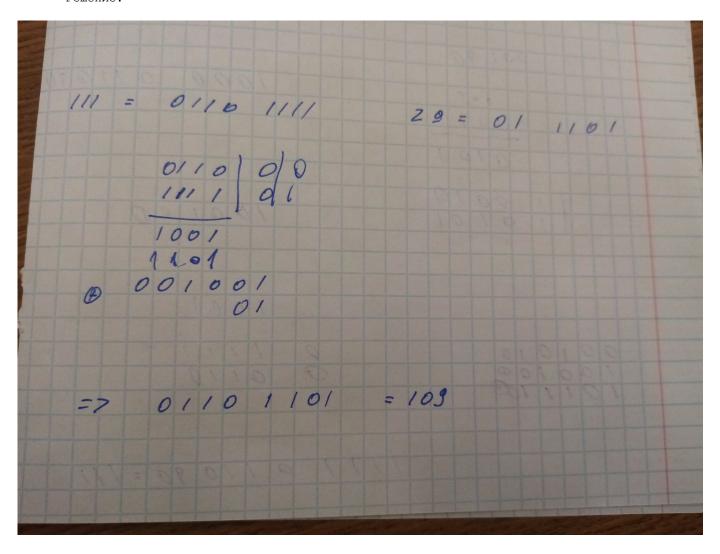
```
... 0b1010111 True
```

Программа:

```
d = 59
pol = 4
n = 3
def crc(d: int, dl: int) ->
                                       int:if ( d < pol):</pre>
                                                                           return d
                                       print(f"{bin(d)}\n{bin(pol << dl)}\n{bin(d ^ (pol << dl) } \n{bin(d ) } \n{b
                                       dl))}\n")return crc(d ^ (pol << dl), dl-1)</pre>
print(crc(59, 3))
   Результат:
                                                    0b111011
                                                                0b100000
```

```
0b11011
0b11011
0b10000
0b1011
0b1011
0b1000
0b11
3
```

Решение:



Результат:

1 бит искажён, оригинальные данные 109

Решение:

```
Sxn: 4
data: 28= 06 01 1100
3, 4, 5 = 011, 100, 101
6. SYN: 0118 100 @ 101= 010 =2
    4 82 = 100 0010 = 110 = 6
  =7 6 64T UCKO X EM.
проверно
          06 111100
      3, 4, 5,6 = 01,100, 101, 110
      011010001010110=100=4
```

Результат:

искажён 6 бит, оригинальные данные 60