МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»
КАФЕДРА №51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

доц., к.т.н.		Окатов А.В
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

ПЕРЕДАЧА ДАННЫХ ПО СКРЫТОМУ КАНАЛУ СВЯЗИ

по курсу: Программно-аппаратные средства защиты информации в инфокоммуникационных системах связи

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР.	5711М		Пятаков В.С.
		подпись, дата	инициалы, фамилия

Санкт-Петербург 2017

Цель работы

Моделирование передачи данных с использование скрытого канала связи.

Порядок выполнения работы

1. Необходимо смоделировать следующие варианты возможных событий передачи пакета данных:.
   1.1. Передачи по скрытому каналу не осуществляется, передача по основному каналу, в котором возникает ошибка.
   1.2. Передачи по скрытому каналу осуществляется, передача по основному каналу без возникновения ошибок.
      1.2.1. Возникает ошибка в одном из блоков триады пакета.
      1.2.2. Возникает ошибка в 2 блоках триады пакета.
2. Сделать по полученным результатам выводы.

Описание выполнения работы

Имеем некоторое сообщение m = 240 бит. Для передачи по каналу связи необходимо добавить к сообщению контрольную сумму. Алгоритм получения контрольной суммы следующий:

Имеем сообщение m и порождающий многочлен g. Максимальная степень порождающего многочлена говорит о длине контрольной суммы. В данной работе используется CRC-16, и для получения её использовался следующий многочлен:

$$g = 1010011010\ 1111001\ ,$$

или в виде многочлена:

$$g(x) = 1 + x^2 + x^5 + x^6 + x^{10} + x^{11} + x^{12} + x^{13} + x^{16}\ .$$

Разделив m на q и взяв остаток от деления, получим контрольную сумму. $m \bmod g = crc$. Итоговый блок содержащий блок данных и контрольную сумму получается путем прибавления одно к другому $message = m + crc$.

Результаты моделирования

Моделирование 1

Представим результат работы программы, которая моделирует систему, где передачи по скрытому каналу не осуществляется, передача по основному каналу, в котором возникает ошибка.

```
                Сгенерировали 3 сообщения длинной 240 бит каждое и обозначили их как m1, m2, m3.

Посчитаем для них контрольные суммы и обозначим их как crc1, crc2, crc3.

Контрольная сумма 1:
crc1=       |0  0  0  0  0  0  0  1  1  1  0  1  0  0  1  0|
Контрольная сумма 2:
crc2=       |1  1  1  0  0  1  0  1  1  1  0  0  1  0  1  0|
Контрольная сумма 3:
crc3=       |0  1  0  1  1  1  0  0  0  0  0  0  0  0  0  1|


Далее передаем наш пакет состоящий из блока данных и измененной контрольной суммой по каналу, в котором есть ошибки.

Полученная контрольная сумма 1:
crc1**=     |0  1  0  0  1  1  0  0  0  1  1  1  0  1  0  1|
Полученная контрольная сумма 2:
crc2**=     |0  0  0  0  1  0  0  0  0  0  1  0  1  1  1  1|
Полученная контрольная сумма 3:
crc3**=     |0  0  1  1  1  1  0  1  1  0  0  0  1  0  1  0|

Сложим по модулю полученную контрольную сумму с пришедшей из канала.

crc1*=      |0  0  0  0  0  0  0  1  1  1  0  1  0  0  1  0|
           +
crc1**=     |0  1  0  0  1  1  0  0  0  1  1  1  0  1  0  1|
           =
            |0  1  0  0  1  1  0  1  1  0  1  0  0  1  1  1|


crc2*=      |1  1  1  0  0  1  0  1  1  1  0  0  1  0  1  0|
           +
crc2**=     |0  0  0  0  1  0  0  0  0  0  1  0  1  1  1  1|
           =
            |1  1  1  0  1  1  0  1  1  1  1  0  0  1  0  1|


crc3*=      |0  1  0  1  1  1  0  0  0  0  0  0  0  0  0  1|
           +
crc3**=     |0  0  1  1  1  1  0  1  1  0  0  0  1  0  1  0|
           =
            |0  1  1  0  0  0  0  1  1  0  0  0  1  0  1  1|
fx >>
```

рисунок 1 - результат работы программы моделирования 1

Один из методов декодирования пакета заключается в том, что можно достать информацию из пакета, посчитать он нее контрольную сумму и сравнить ее с пришедшей в пакете, если сумма по модулю два равна 0 , это значит что ошибок не произошло.

Из полученного в ходе моделирования результата можно видеть, что все контрольные суммы различаются и сумма по модулю два с пришедшей из канала дает разные результаты, что говорит о том, что в канале были ошибки.

Моделирование 2

Представим результат работы программы, которая моделирует систему, где осуществляется передача по скрытому каналу , передача по основному каналу происходит без ошибок.

```
                Сгенерировали 3 сообщения длинной 240 бит каждое и обозначили их как m1, m2, m3.

Посчитаем для них контрольные суммы и обозначим их как crc1, crc2, crc3.

Контрольная сумма 1:
crc1=       |0  0  0  1  0  0  0  1  0  0  1  0  0  1  1  0|
Контрольная сумма 2:
crc2=       |0  1  1  0  0  1  0  1  0  0  0  1  0  1  1  0|
Контрольная сумма 3:
crc3=       |1  0  1  0  1  1  1  0  1  1  1  1  1  1  1  1|

Внесем в наши контрольные суммы секретную информацию.
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|

После внесения секретной информации получим следующие измененные контрольные суммы crc1*,crc2*,crc3*:

Контрольная сумма 1:
crc1=       |0  0  0  1  0  0  0  1  0  0  1  0  0  1  1  0|
          +
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|
          =
crc1*=      |1  0  0  1  0  0  0  1  0  0  1  0  0  1  1  0|

Контрольная сумма 2:
crc2=       |0  1  1  0  0  1  0  1  0  0  0  1  0  1  1  0|
          +
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|
          =
crc2*=      |1  1  1  0  0  1  0  1  0  0  0  1  0  1  1  0|

Контрольная сумма 3:
crc3=       |1  0  1  0  1  1  1  0  1  1  1  1  1  1  1  1|
          +
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|
          =
crc3*=      |0  0  1  0  1  1  1  0  1  1  1  1  1  1  1  1|
```

рисунок 2 - результат работы программы моделирования 2 (а)

```
Далее передаем наш пакет состоящий из блока данных и измененной контрольной суммой по каналу, в котором нет ошибок.
Выделим полученные данные, обозначенные как m1*,m2*,m3* и посчитаем от них контрольные суммы crc1**,crc2**,crc3**.

Полученная контрольная сумма 1:
crc1**=     |0  0  0  1  0  0  0  1  0  0  1  0  0  1  1  0|
Полученная контрольная сумма 2:
crc2**=     |0  1  1  0  0  1  0  1  0  0  0  1  0  1  1  0|
Полученная контрольная сумма 3:
crc3**=     |1  0  1  0  1  1  1  0  1  1  1  1  1  1  1  1|

Сложим по модулю полученную контрольную сумму с пришедшей из канала.

crc1*=      |1  0  0  1  0  0  0  1  0  0  1  0  0  1  1  0|
           +
crc1**=     |0  0  0  1  0  0  0  1  0  0  1  0  0  1  1  0|
           =
            |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|


crc2*=      |1  1  1  0  0  1  0  1  0  0  0  1  0  1  1  0|
           +
crc2**=     |0  1  1  0  0  1  0  1  0  0  0  1  0  1  1  0|
           =
            |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|


crc3*=      |0  0  1  0  1  1  1  0  1  1  1  1  1  1  1  1|
           +
crc3**=     |1  0  1  0  1  1  1  0  1  1  1  1  1  1  1  1|
           =
            |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|
fx >>
```

рисунок 3 - результат работы программы моделирования 2 (б)

Из полученного в ходе моделирования результата можно видеть, что все контрольные суммы различаются и сумма по модулю два с пришедшей из канала дает одинаковые результаты, что говорит о том, что мы передавали информацию по скрытому каналу связи, сделав этот вывод по правилу мажоритарности.

Моделирование 3

Представим результат работы программы, которая моделирует систему, где осуществляется передача по скрытому каналу , передача по основному каналу происходит с ошибкой в одном блоке данных.

```
                    Сгенерировали 3 сообщения длинной 240 бит каждое и обозначили их как m1, m2, m3.

Посчитаем для них контрольные суммы и обозначим их как crc1, crc2, crc3.

Контрольная сумма 1:
crc1=       |0  0  1  0  0  1  0  0  1  1  0  0  1  1  0  1|
Контрольная сумма 2:
crc2=       |0  0  0  0  0  0  1  1  1  1  0  1  0  1  1  1|
Контрольная сумма 3:
crc3=       |0  1  1  0  0  1  0  0  1  0  1  1  0  1  0  0|

Внесем в наши контрольные суммы секретную информацию.
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|

После внесения секретной информации получим следующие измененные контрольные суммы crc1*,crc2*,crc3*:

Контрольная сумма 1:
crc1=       |0  0  1  0  0  1  0  0  1  1  0  0  1  1  0  1|
           +
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|
           =
crc1*=      |1  0  1  0  0  1  0  0  1  1  0  0  1  1  0  1|

Контрольная сумма 2:
crc2=       |0  0  0  0  0  0  1  1  1  1  0  1  0  1  1  1|
           +
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|
           =
crc2*=      |1  0  0  0  0  0  1  1  1  1  0  1  0  1  1  1|

Контрольная сумма 3:
crc3=       |0  1  1  0  0  1  0  0  1  0  1  1  0  1  0  0|
           +
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|
           =
crc3*=      |1  1  1  0  0  1  0  0  1  0  1  1  0  1  0  0|
```

рисунок 4 - результат работы программы моделирования 3 (а)

```
Далее передаем наш пакет состоящий из блока данных и измененной контрольной суммой по каналу,
в котором происходит ошибки, и допустим ошибка была в первом блоке данных.
Выделим полученные данные, обозначенные как m1*,m2*,m3* и посчитаем от них контрольные суммы crc1**,crc2**,crc3**.

Полученная контрольная сумма 1:
crc1**=     |1  0  0  0  0  0  1  0  0  1  1  1  0  0  0  1|
Полученная контрольная сумма 2:
crc2**=     |0  0  0  0  0  0  1  1  1  1  0  1  0  1  1  1|
Полученная контрольная сумма 3:
crc3**=     |0  1  1  0  0  1  0  0  1  0  1  1  0  1  0  0|

Сложим по модулю полученную контрольную сумму с пришедшей из канала.

crc1*=      |1  0  1  0  0  1  0  0  1  1  0  0  1  1  0  1|
           +
crc1**=     |1  0  0  0  0  0  1  0  0  1  1  1  0  0  0  1|
           =
            |0  0  1  0  0  1  1  0  1  0  1  1  1  1  0  0|


crc2*=      |1  0  0  0  0  0  1  1  1  1  0  1  0  1  1  1|
           +
crc2**=     |0  0  0  0  0  0  1  1  1  1  0  1  0  1  1  1|
           =
            |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|


crc3*=      |1  1  1  0  0  1  0  0  1  0  1  1  0  1  0  0|
           +
crc3**=     |0  1  1  0  0  1  0  0  1  0  1  1  0  1  0  0|
           =
            |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|
>> |
```

рисунок 5 - результат работы программы моделирования 3 (б)

Из полученного в ходе моделирования результата можно видеть, что все контрольные суммы различаются и сумма по модулю два с пришедшей из канала дает одинаковые результаты, но только для двух блоков данных, что говорит о том, что мы передавали информацию по скрытому каналу связи, сделав этот вывод по правилу мажоритарности, но при этом в первом блоке произошла ошибка, так как его сумма отличается от двух других.

Моделирование 4

Представим результат работы программы, которая моделирует систему, где осуществляется передача по скрытому каналу , передача по основному каналу происходит с ошибкой в двух блоках данных.

```
                Сгенерировали 3 сообщения длинной 240 бит каждое и обозначили их как m1, m2, m3.

Посчитаем для них контрольные суммы и обозначим их как crc1, crc2, crc3.

Контрольная сумма 1:
crc1=       |0  0  1  1  1  1  1  0  1  0  0  1  0  0  1  1|
Контрольная сумма 2:
crc2=       |0  0  0  1  1  1  0  1  0  0  1  1  0  1  0  0|
Контрольная сумма 3:
crc3=       |0  0  0  1  1  1  1  0  0  1  1  1  1  0  1  0|

Внесем в наши контрольные суммы секретную информацию.
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|

После внесения секретной информации получим следующие измененные контрольные суммы crc1*,crc2*,crc3*:

Контрольная сумма 1:
crc1=       |0  0  1  1  1  1  1  0  1  0  0  1  0  0  1  1|
          +
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|
          =
crc1*=      |1  0  1  1  1  1  1  0  1  0  0  1  0  0  1  1|

Контрольная сумма 2:
crc2=       |0  0  0  1  1  1  0  1  0  0  1  1  0  1  0  0|
          +
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|
          =
crc2*=      |1  0  0  1  1  1  0  1  0  0  1  1  0  1  0  0|

Контрольная сумма 3:
crc3=       |0  0  0  1  1  1  1  0  0  1  1  1  1  0  1  0|
          +
секр.инф=   |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|
          =
crc3*=      |1  0  0  1  1  1  1  0  0  1  1  1  1  0  1  0|
```

рисунок 6 - результат работы программы моделирования 4 (а)

```
Далее передаем наш пакет состоящий из блока данных и измененной контрольной суммой по каналу,
в котором происходит ошибки, и допустим ошибка была в первом блоке данных и в третьем.
Выделим полученные данные, обозначенные как m1*,m2*,m3* и посчитаем от них контрольные суммы crc1**,crc2**,crc3**.

Полученная контрольная сумма 1:
crc1**=     |1  0  0  1  1  0  0  0  0  0  1  0  1  1  1  1|
Полученная контрольная сумма 2:
crc2**=     |0  0  0  1  1  1  0  1  0  0  1  1  0  1  0  0|
Полученная контрольная сумма 3:
crc3**=     |0  0  0  1  0  1  0  1  0  0  1  1  1  1  0  1|

Сложим по модулю полученную контрольную сумму с пришедшей из канала.

crc1*=      |1  0  1  1  1  1  1  0  1  0  0  1  0  0  1  1|
           +
crc1**=     |1  0  0  1  1  0  0  0  0  0  1  0  1  1  1  1|
           =
            |0  0  1  0  0  1  1  0  1  0  1  1  1  1  0  0|


crc2*=      |1  0  0  1  1  1  0  1  0  0  1  1  0  1  0  0|
           +
crc2**=     |0  0  0  1  1  1  0  1  0  0  1  1  0  1  0  0|
           =
            |1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0|


crc3*=      |1  0  0  1  1  1  1  0  0  1  1  1  1  0  1  0|
           +
crc3**=     |0  0  0  1  0  1  0  1  0  0  1  1  1  1  0  1|
           =
            |1  0  0  0  1  0  1  1  0  1  0  0  0  1  1  1|
fx >>
```

рисунок 7 - результат работы программы моделирования 4 (б)

Из полученного в ходе моделирования результата можно видеть, что все контрольные суммы различаются и сумма по модулю два с пришедшей из канала дает разные результаты, для всех блоков данных, что говорит о том, что мы не можем достоверно утверждать, передавалась информация по скрытому каналу или нет, так как значения сумм пришедшей контрольной суммы и из пакета отличаются.

Выводы

В ходе выполнения лабораторной работы были реализованы 4 алгоритма моделирования передачи информации по основным и скрытым каналам связи.

По полученным результатам моделирования можно сделать следующие выводы:

При передаче по основному каналу связи и без внесение секретной информации, на приемной стороне не возможно определить какая секретная информация передавалась и передавались ли вообще, если проходя через канал блок данных изменился.

При передаче по основному каналу связи и с внесением секретной информации в контрольную сумму, на приемной стороне сможешь безошибочно достать секретную информацию, если в канале не происходит ошибок. Так как сумма по модулю 2 посчитанной контрольной суммы от принятого блока данных и контрольной суммы пришедшей из канала будут давать одинаковый результат для всех блоков данных из пакета, по этому по правилу мажоритарности принимаем решение о том, что передавалась секретная информация по скрытому каналу связи.

При передачи по основному каналу связи и с добавлением секретной информации в контрольную сумму, на приемной стороне будем наблюдать следующую картину, при условии что ошибки возникли только в одном из 3 блоков данных. Два блока данных в которых не происходили ошибки, дадут контрольные суммы при сложении по модулю два с которыми, контрольные суммы пришедшие из канала дадут одинаковый результат. Блок данных в котором произошли ошибки напротив даст какой-то другой результат. Но сравнивая три полученных суммы, можем заметить что так как две одинаковые, то по правилу можоритарности, делаем вывод о том, что передавалась секретная информация, но в одном блоке данных произошла ошибка.

При передачи по основному каналу связи и с добавлением секретной информации в контрольную сумму, на приемной стороне будем наблюдать следующую картину, при условии, что ошибки возникли в 2 из 3 блоке данных. Каждый блока данных даст разные результаты, и обнаружить передачу по скрытому каналу будет невозможно.

ПРИЛОЖЕНИЕ

Листинг программ реализующих моделирования

Моделирование 1

```
close all;
clear all;
clc;
q=[1 0 1 0 0 1 1 0 1 0 1 1 1 1 0 0 1];%порождающий многочлен
d=256;% общая длина сообщения
m=randi(0:1,3,d-length(q)+1);%случ сообщение
 [ m1,crc1 ] = CRC( m(1,:),q,d );
[ m2,crc2 ] = CRC( m(2,:),q,d );
[ m3,crc3 ] = CRC( m(3,:),q,d );
m1=m1(1,17:end);
m2=m2(1,17:end);%240
m3=m3(1,17:end);
error=randi(0:1,1,240);
m1=mod(m1+error,2);
error1=randi(0:1,1,240);
m2=mod(m2+error1,2);
error3=randi(0:1,1,240);
m3=mod(m3+error3,2);
crc1=crc1(1,1:16);
crc2=crc2(1,1:16);%16
crc3=crc3(1,1:16);
[ m1_1,crc1_1 ] = CRC( m1,q,d );
[ m2_2,crc2_2 ] = CRC( m2,q,d );%приняли и посчитал контрольную сумму от
принятого
[ m3_3,crc3_3 ] = CRC( m3,q,d );
crc1_1=crc1_1(1,1:16);
crc2_2=crc2_2(1,1:16);%16
crc3_3=crc3_3(1,1:16);
secret1=mod(crc1+crc1_1,2);
secret2=mod(crc2+crc2_2,2);
secret3=mod(crc3+crc3_3,2);
```

Моделирование 2

```
close all;
clear all;
clc;
q=[1 0 1 0 0 1 1 0 1 0 1 1 1 1 0 0 1];%порождающий многочлен
d=256;% общая длина сообщения
m=randi(0:1,3,d-length(q)+1);%случ сообщение
[ m1,crc1 ] = CRC( m(1,:),q,d );
[ m2,crc2 ] = CRC( m(2,:),q,d );
[ m3,crc3 ] = CRC( m(3,:),q,d );
m1=m1(1,17:end);
m2=m2(1,17:end);%240
m3=m3(1,17:end);
crc1=crc1(1,1:16);
crc2=crc2(1,1:16);%16
crc3=crc3(1,1:16);
sec_chanel=[1,zeros(1,length(crc1)-1)];% секр. инф
crc1=mod(crc1+sec_chanel,2);
```

```
crc2=mod(crc2+sec_chanel,2);
crc3=mod(crc3+sec_chanel,2);
 [ m1_1,crc1_1 ] = CRC( m1,q,d );
[ m2_2,crc2_2 ] = CRC( m2,q,d );%приняли и посчитал контрольную сумму от
принятого
[ m3_3,crc3_3 ] = CRC( m3,q,d );
crc1_1=crc1_1(1,1:16);
crc2_2=crc2_2(1,1:16);%16
crc3_3=crc3_3(1,1:16);
secret1=mod(crc1+crc1_1,2);
secret2=mod(crc2+crc2_2,2);
secret3=mod(crc3+crc3_3,2);
```

Моделирование 3

```
close all;
clear all;
clc;
q=[1 0 1 0 0 1 1 0 1 0 1 1 1 1 0 0 1];%порождающий многочлен
d=256;% общая длина сообщения
m=randi(0:1,3,d-length(q)+1);%случ сообщение
[ m1,crc1 ] = CRC( m(1,:),q,d );
[ m2,crc2 ] = CRC( m(2,:),q,d );
[ m3,crc3 ] = CRC( m(3,:),q,d );
m1=m1(1,17:end);
m2=m2(1,17:end);%240
m3=m3(1,17:end);
error=[1,zeros(1,239)];%ошибка в канале
m1=mod(m1+error,2);
crc1=crc1(1,1:16);
crc2=crc2(1,1:16);%16
crc3=crc3(1,1:16);
sec_chanel=[1,zeros(1,length(crc1)-1)];% секр. инф
crc1=mod(crc1+sec_chanel,2);
crc2=mod(crc2+sec_chanel,2);
crc3=mod(crc3+sec_chanel,2);
 [ m1_1,crc1_1 ] = CRC( m1,q,d );
[ m2_2,crc2_2 ] = CRC( m2,q,d );%приняли и посчитал контрольную сумму от
принятого
[ m3_3,crc3_3 ] = CRC( m3,q,d );
crc1_1=crc1_1(1,1:16);
crc2_2=crc2_2(1,1:16);%16
crc3_3=crc3_3(1,1:16);
secret1=mod(crc1+crc1_1,2);
secret2=mod(crc2+crc2_2,2);
secret3=mod(crc3+crc3_3,2);
```

Моделирование 4

```
close all;
clear all;
clc;
q=[1 0 1 0 0 1 1 0 1 0 1 1 1 1 0 0 1];%порождающий многочлен
d=256;% общая длина сообщения
m=randi(0:1,3,d-length(q)+1);%случ сообщение
[ m1,crc1 ] = CRC( m(1,:),q,d );
[ m2,crc2 ] = CRC( m(2,:),q,d );
[ m3,crc3 ] = CRC( m(3,:),q,d );
m1=m1(1,17:end);
m2=m2(1,17:end);%240
m3=m3(1,17:end);
```

```
error=[1,zeros(1,239)];%ошибка в канале 1 пает
m1=mod(m1+error,2);
error1=[zeros(1,239),1];%ошибка в канале 3 пакет
m3=mod(m3+error1,2);
crc1=crc1(1,1:16);
crc2=crc2(1,1:16);%16
crc3=crc3(1,1:16);
sec_chanel=[1,zeros(1,length(crc1)-1)];% секр. инф
crc1=mod(crc1+sec_chanel,2);
crc2=mod(crc2+sec_chanel,2);
crc3=mod(crc3+sec_chanel,2);
 [ m1_1,crc1_1 ] = CRC( m1,q,d );
[ m2_2,crc2_2 ] = CRC( m2,q,d );%приняли и посчитал контрольную сумму от
принятого
[ m3_3,crc3_3 ] = CRC( m3,q,d );
crc1_1=crc1_1(1,1:16);
crc2_2=crc2_2(1,1:16);%16
crc3_3=crc3_3(1,1:16);
secret1=mod(crc1+crc1_1,2);
secret2=mod(crc2+crc2_2,2);
secret3=mod(crc3+crc3_3,2);
```

Функция для вычисления контрольной суммы

```
 function [ p,a ] = CRC( m,q,d )

for i=length(q):-1:1
    if q(1,i)==1
        if i>xr
        xr=i-1;
        else
       break;
        end
    end
end
%%
%% перевод в размерность как a , для деления
q1=zeros(1,d);
for i=1:1:d
    if i>length(q)
        q1(1,i)=0;
    else
 q1(1,i)=mod(q(1,i)+q1(1,i),2);

    end
end
%% m(x)*x^r
a=zeros(1,d);
for i=1:1:length(m)
    if m(1,i)==1
        a(1,i+xr)=1;
    end
end
p=a;
n=d;%для определения макс степени для многочлена
sdvig=d;%это мол шаг в столбике
 for i=d:-1:1
       if sdvig~=0%пока степень m(x)*x^r и степень многослена не будут равны,
ну или их ращница нулю
        if a(1,i)==1%проверяем каждую ячейку
            deg_a=i;%считали степень
                    while q1(1,n)~=1
```

```
                        n=n-1;
                    end
                deg_q=n;%посчитали степень у порождающего
                sdvig=deg_a-deg_q;%оценили сдвиг ну тип это по столбику на что
умножит чтобы получить многочлен чтобы потом сложить с исзодным
                if sdvig>=0
                b=zeros(1,d);%промежуточный этапчик
        for j=1:1:length(q1)
            if q1(1,j)==1
                b(1,j+sdvig)=1;%вот это то что получается когда делимое
умножаешь на элемент частного, с чем потом будет вычитать делитель
            end
        end
          a=mod(a+b,2);%вот сложили получили то что после вычитания и это уже
бужем делить на порождающий
                end
        end
       %когда все пройдем последний а это остаток он и будет нашей кс
       else
           break;
       end
 end
a1=mod(p+a,2);
end
```