МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Н.И. ЛОБАЧЕВСКОГО»

РАДИОФИЗИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Научно-исследовательская работа

Работу выполнил: студент

Группы \_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_ Гусев Ю.С.

(подпись)

Номер зачётной книжки

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Проверил:

\_\_\_\_\_\_\_\_\_\_\_ Горбунов А.А.

(подпись)

Н. Новгород, 2018

Содержание

[1. Введение 3](#__RefHeading___Toc1373_557217930)

[2. Модель криптосистемы на основе частотного подхода 4](#__RefHeading___Toc1375_557217930)

[3. Схема шифрования методом гаммирования](#__RefHeading___Toc1381_557217930) 5

[3.1 Частотный подход к реализации автомата 6](#__RefHeading___Toc1383_557217930)

[3.2. Обратное z-преобразование……………………………………….7](#__RefHeading___Toc1389_557217930)

[4. Реализация на языке программирования 9](#__RefHeading___Toc1389_557217930)

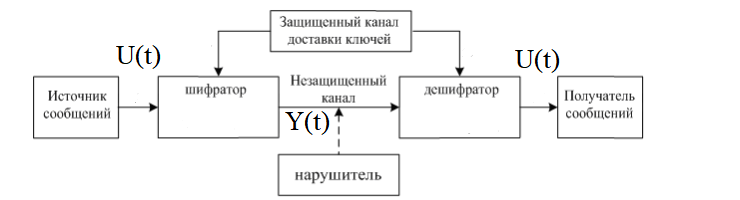
5. Листинг программы………………………………………………...12

[6. Заключение](#__RefHeading___Toc1391_557217930) 15

[7. Список литературы](#__RefHeading___Toc2038_557217930) 16

**1. Введение**

Криптографическая система – это набор различных преобразований или алгоритмов над входящим сообщением для его последующей защиты при передаче по незащищенному каналу связи. Обобщенная модель такой системы представлена на следующем рисунке:



По защищенному каналу передается ключ, с помощью которого происходит однозначное шифрование и дешифрование сообщения.

Для описание дискретных устройств, реализующих отдельные операции шифрования и дешифрования криптосистемы (далее КС) применена теория линейных цифровых автоматов (далее ЛЦА). Для алгоритмического описания ЛЦА возможно использовать два способа – временной и частотный.

В данной работе будут реализованы модели шифратора и дешифратора криптосистемы с использованием частотного подхода.

**2. Модель криптосистемы на основе частотного подхода.**

Пусть U(t) – дискретный сигнал, поступающий на вход шифратора.

Обозначим за Y(t) дискретный зашифрованный сигнал, поступающий с выхода шифратора.

Шифратор можно представить в виде системы линейных уравнений на языке ABCD-формализма:

, где A, B, C, D – матрицы **(2.1)**

Если ∃ D-1 и A\*=[A-BD-1C], B\*=[BD-1] , C\*=[-D-1C] , D\*=[D-1] , x0\* = x0 , то из автомата порождающего можно построить восстанавливающий автомат, а именно дешифратор:

**(2.2)**

При такой модели в роли ключа выступают матричные параметры A, B, C, D, x0 , которые будут передаваться по закрытому каналу связи.

При частотном методе описания используется z-преобразование

U(z)=

Таким образом, уравнения СЛУ (1) изменяются по закону:

u(t) ⇒ U(z), y(t) ⇒ Y(z), x(t) ⇒ X(z), x(t+1) ⇒ AX(z)+BU(z), Y(z)=CX(z)+DU(z)

K1(z)=C(zE-A)-1B+D, K2(z)=zC(zE-A)-1 ⇒ Y(z)=K1U(z)+ K2x0

Аналогичные преобразования выполняются для дешифратора и получается соотношение:  
Y\*(z)=K1\*(z)U\*(z)+ K2\*(z)x0, где K1\*(z)=C\* (zE-A\*)-1B\*+D\*, K2\* (z)=zC\* (zE-A\*)-1 **(2.3)**

Условие восстановления сообщения выглядит следующим образом:

K1\*(z)= K1(z)-1, K2\*(z)= K2(z)-1, x0=x0\*.

**3. Схема шифрования методом гаммирования.**

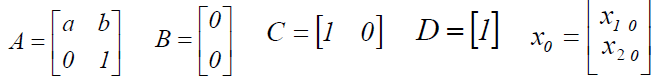
В данном методе шифрование исходного сообщения происходит путем его сложения с гаммой по модулю, равному размерности алфавита исходного сообщения.

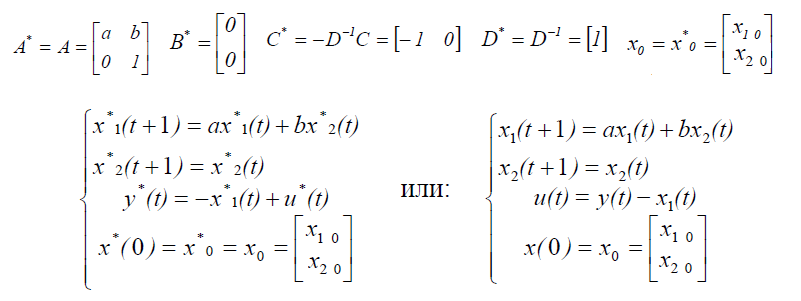
Гамма – это псевдослучайная последовательность чисел, порождаемая каким-либо алгоритмом.

В данной работе для получения гамма будет использован линейный конгруэнтный метод, а система уравнений, описывающая шифратор, будет иметь следующий вид:

**(3.1)**

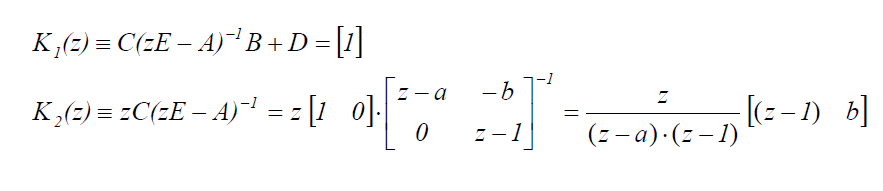
Матрицы будут иметь следующий вид:



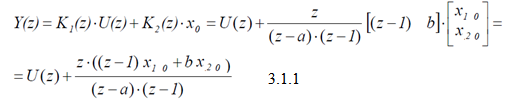
Соответственно, для дешифратора:  


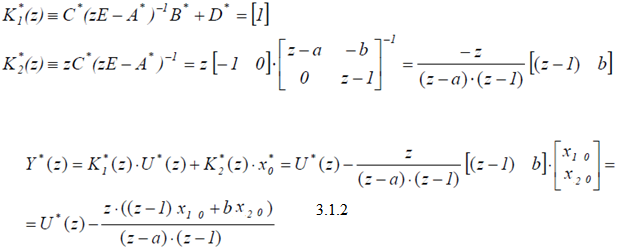
**3.1 Частотный подход к реализации автомата.**

После проведения z-преобразования над коэффициентами передачи (2.3) и подстановки соответствующих значений матриц получим следующие выражения коэффициентов:



Конечное выражение для выходного сигнала (2.3) будет иметь вид:

  
  
 Соответственно, для дешифратора:



**3.2. Обратное z-преобразование.**

Z-преобразование от входного сигнала u(t) по сути своей представляет следующее выражение.

Таким образом, выражение выходного сигнала на шифраторе на частотном языке для конкретного значения входного сигнала в момент времени n будет иметь вид **(3.2.1)**:

Для выходного сигнала дешифратора (входного для шифратора) **(3.2.2.)**:

Что бы получить из выражений **3.2.1.** и **3.2.2** сигналы в исходной форме, то есть дискретные по времени, нужно провести обратное z-преобразование над полученными выражениями.

Существуют несколько способов обратного преобразования:

1) Взять напрямую интеграл через вычеты

2) Разложением н простые дроби

3) Делением числителя на знаменатель

4) Разложением в степенной ряд

Для реализации алгоритма на языке программирования наиболее удобным является способ через вычеты, поэтому далее рассмотрим его подробнее.

Отсюда следует, что

Видно, что уравнение имеет три особые точки

Все точки являются полюсами первого порядка, так как предел выражения при стремлении z к любой из них – бесконечность.

Таким образом,

так как сложение происходит по модулю размерности алфавита.

Для дешифратора уравнение примет вид:

**4. Реализация на языке программирования.**

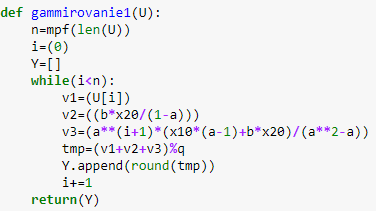
Для написания программы был выбран язык программирования

Python 3 как наиболее простой и понятный для меня.

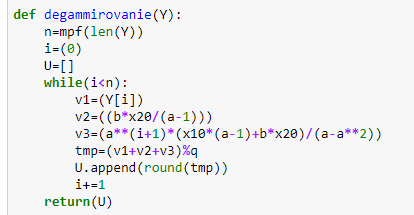
Полный листинг программы можно найти в пункте ХУЙ, здесь же будет приведено описание отдельных ее элементов и примеры функционирования.

Были написаны три варианта функции, реализующей шифрование – два на через z-преобразование и один с помощью системы уравнений **(3.1)**.

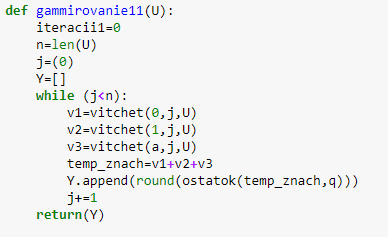
Функция **gammirovanie1** реализует данный процесс, используя выражение



Функция **degammirovanie** реализует дешифратор, используя выражение



Функция **gammirovanie11** в результате делает то же самое, но используя дополнительную функцию **vitchet** для расчета значений вычетов в особых точках.

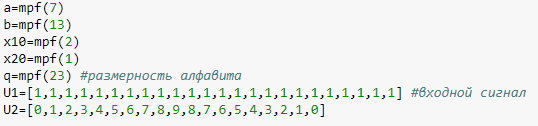


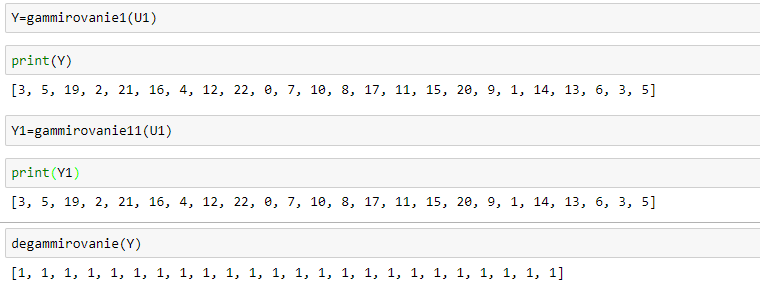
Функции **K2\_chislitel**, **K2\_znamenatel**, **K2\_znamenatel\_d** реализуют соответственно числитель, знаменатель и производную знаменателя дроби из выражения 3.1.1.

Функция на основе системы **(3.1)** быланаписана с целью проверки работоспособности основного алгоритма, так как является более простой в реализации и не требует высокой точности вычислений, в отличии от функций **gammirovanie11, gammirovanie1, degammirovanie**.

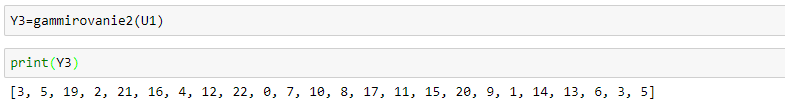
Далее приведены примеры работоспособности программы:

Начальные параметры

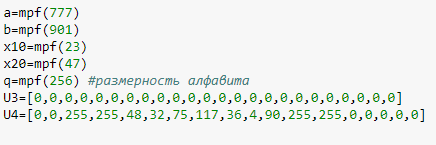


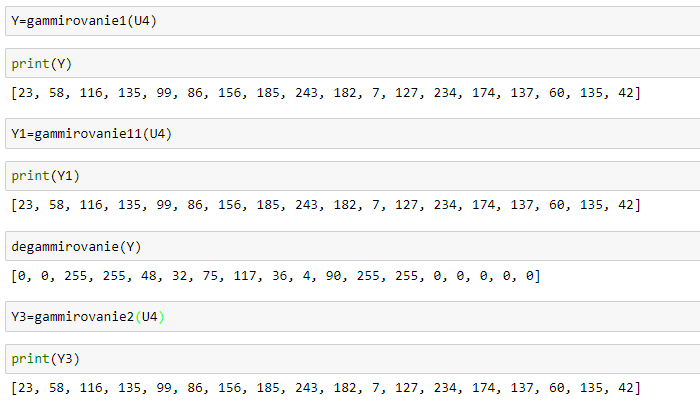


Сравним с результатом функции **gammirovanie2**

  
Результаты совпадают, а значит, алгоритм работает верно.

Проверим работу для других начальных данных:





**5. Листинг программы.**







**6. Заключение.**

Были рассмотрены различные методы шифрования, а так же один из них был реализован различными способами, проведены тесты работоспособности и сравнение результатов.

В процессе написания алгоритма выяснилось, что способ с использованием z-преобразования является не самым простым и удобным, так как пришлось придумывать, как реализовать обратное z-преобразование, а в последствии я столкнулся с тем, что данный метод требует большой точности вычислений (70 знаков после запятой), так как в противном случае происходила потеря не только дробных частей, но и знаков до запятой.

В перспективе нужно провести анализ сложности данного метода шифрования и различных способов его реализации для сравнения, например, с, например, алгоритмами Вижинера и Цезаря, чтобы понять, имеются ли какие-нибудь преимущества данного варианта, а так же возможно сделать алгоритм более универсальным, чтоб была возможность использовать различные псевдослучайные генераторы.

**7. Список литературы.**

1) ДИНАМИЧЕСКИЕ МОДЕЛИ КРИПТОСИСТЕМ С ЗАКРЫТЫМ КЛЮЧОМ. СИНТЕЗ ДЕШИФРАТОРОВ А.А.Горбунов, К.Г.Кирьянов

2) Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов. М: Мир, 1978.

3) Материал энциклопедии Википедия по теме Z-преобразование