ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ИНФОРМАЦИОННОГО ОБМЕНА ПО НЕЗАЩИЩЕННОМУ КАНАЛУ СВЯЗИ

Аннотация

Информационный обмен представляет собой обмен информацией между двумя и более абонентами и подразумевает передачу сообщений (текста) по каналам связи. В современном мире отправляемая по разным каналам связи информация представлена в цифровом виде. Это означает, что передаче не непрерывным (аналоговый) сигналом, а последовательность целых чисел n1, n2, n3.... которые принимают значения из некоторого фиксированного конечного интервала. Эти числа называемые символами, поступают от источника информации с периодом T, а частота, соответствующая этому периоду, называется символьной скоростью. Символы определяет алфавит, применяемый в системе передачи информации. Часто используемым на практике вариантом алфавита является бинарный алфавит, формирующий двоичную последовательность символов (каждое ni может принимать значение 0 и 1).

Системы цифровой связи становятся все более востребованы, вследствие постоянно растущего спроса и из-за того, что цифровая передача предлагает возможности обработки информации, не доступные при использовании аналоговой передачи. Одной из главных отличительной особенностью систем цифровой связи является то, что за конечный промежуток времени они посылают сигнал, состоящий из конечного набора элементарных сигналов. В системах цифровой связи задачей приемника является не точное воспроизведение переданного сигнала, а определение на основе искаженного шумами сигнала, какой именно сигнал из конечного набора был послан передатчиком.

Главным преимуществом цифровой связи является легкость восстановления цифровых сигналов по сравнению с аналоговыми. Цифровые каналы меньше подвержены искажению и интерференции, чем аналоговые. Цифровые каналы более надежны и могут производиться по более низким ценам, чем аналоговые. Кроме того, цифровое программное обеспечение допускает более гибкую реализацию, чем аналоговое. При передаче и коммутации различные типы цифровых сигналов могут рассматриваться как идентичные: ведь бит — это и есть бит. Кроме того, для удобства коммутации и обработки, цифровые сообщения могут группироваться в автономные единицы, называемые пакетами. В цифровые технологии естественным образом внедряются функции, защищающие от интерференции и подавления сигнала, либо обеспечивающие шифрование или секретность.

# 1 Постановка задачи

Цель выполнения курсовой работы является подготовка к деятельности, связанной с особенностями обеспечения безопасного информационного обмена, закрепление и практическое применение знаний методов защиты информации, передаваемой по незащищенным каналам связи, полученных в процессе изучения курса «Модели и методы безопасного информационного обмена».

Задачи работы:

* разработка подсистемы преобразование передаваемой информации в цифровой вид;
* разработка подсистемы шифрования и дешифрования передаваемой информации;
* разработка подсистемы модуляции и демодуляции передаваемого сообщения;
* иллюстрация последовательности выполняемых преобразований в процессе;
* сеанса безопасного информационного обмена.

# 1.1 Описание исходных данных

Исходный текст - сообщение «a snake lurks in the grass ». Открытое сообщение, которое будет использовано для проведения операций кодирования, декодирования и модуляции сигнала.

Исходные данные аналоговой модуляции с использованием амплитудной манипуляции несущего колебания:

*f (t) Asin(t):* $ω$*= 106;* $A\_{1}$ *= 16;* $A\_{0}$ *= 11.*

# 1.2 Основные этапы передачи информации

Информация передается в виде сигналов. Сигнал есть физический процесс, несущий в себе информацию. Сигнал может быть звуковым, световым и др. Наиболее распространен сигнал в электрической форме, определяющийся функциональной схемой (рисунок 1).



Рисунок 1 – Функциональная схема типичной системы цифровой связи.

Этапы обработки сигнала, имеющие место в передатчике, являются преимущественно обратными к этапам приемника. На рис. 1 исходная информация преобразуется в двоичные цифры (биты); после этого биты группируются в цифровые сообщения или символы сообщенийДля систем, использующих канальное кодирование (коды коррекции ошибок), последовательность символов сообщений преобразуется в последовательность канальных символов (кодовых символов), и каждый канальный символ обозначается ui. Поскольку символы сообщений или канальные символы могут состоять из одного бита или группы битов, последовательность подобных символов называется потоком битов.

Рассмотрим ключевые блоки обработки сигналов, изображенные на рисунке 1.

Необходимыми для систем цифровой связи являются этапы:

* форматирования;
* модуляции;
* демодуляции и детектирования;
* синхронизации.

Кроме того, для обеспечения безопасного информационного обмена важным элементом системы связи является наличие этапа шифрования/дешифрования информации, обеспечивающих конфиденциальность связи.

Форматирование преобразовывает исходную информацию в биты, обеспечивая, таким образом, совместимость информации и функций обработки сигналов с системой цифровой связи. С этой точки рисунка и вплоть до блока импульсной модуляции информация остается в форме потока битов.

Модуляция – это процесс, посредством которого символы сообщений или канальные символы (если используется канальное кодирование) преобразуются в сигналы, совместимые с требованиями, налагаемыми каналом передачи данных.

Для систем передачи радиочастотного диапазона следующим важным этапом является полосовая модуляция; она необходима всегда, когда среда передачи не поддерживает распространение сигналов, имеющих форму импульсов. В таких случаях среда требует полосового сигнала si(t), где i = 1,...,M. Термин «полосовой» используется для отражения того, что видеосигнал $g\_{i}(t)$ сдвинут несущей волной на частоту, которая гораздо больше частоты спектральных составляющих. Далее сигнал $s\_{i}(t)$ проходит через канал, причем связь между входным и выходным сигналами канала полностью определяется импульсной характеристикой канала. Демодуляция обычно выполняется с помощью опорных сигналов.

Синхронизация предназначена для координирования действий, выполняемых в процессе передачи информации и может выполняться для пяти параметров, определяющих её вид. Соответственно, частотная синхронизация, фазовая синхронизация, символьная синхронизация, кадровая синхронизация, сетевая синхронизация. Основной процесс синхронизации по времени – это символьная синхронизация, необходимая для определения демодулятором и детектором начала и конца процесса детектирования символа и бита. Ошибка в данном случае приведет к снижению эффективности детектирования. Синхронизация по времени предназначена для кадровой синхронизации и позволяет перестраивать сообщения. Синхронизация и ее ключевой элемент, синхронизирующий сигнал, задействованы во всех этапах обработки сигнала в системе. Для простоты блок синхронизации на рисунке 1 показан безотносительно к чему-либо, хотя фактически он участвует в регулировании операций практически в каждом блоке.

Шифрование и дешифрование – это преобразования передаваемых по каналу связи сообщений, проводимые соответственно передатчиком и приемником информации. Шифрование используется для обеспечения секретности связи, предотвращает понимание сообщения несанкционированным пользователем и введение в систему ложных сообщений. В данной работе применяется алгоритмов блочного симметричного шифрования, он заключается в преобразования шифры подстановки (замены) и шифры перестановки (транспозиции).

Шифр подстановки – преобразований заключается в замене символа исходного текста на другие символы (того же алфавита) по более или менее сложному правилу. Один из первых шифров, «Шифр Цезаря» в нем каждая буква алфавита заменяется буквой, которая находиться на k-той позиции в этом же алфавите.

Шифр перестановки – преобразование строиться на использовании перестановок букв открытого текста. Принцип шифрование представляет собой, запись текста сообщения в горизонтальные строки одинаковой длины и последующее считывание текста столбец за столбцом, но не порядку, а в соответствии с некоторой перестановкой столбцов. Порядок считывания столбцов при этом становится ключом алгоритма.

# 2 Описание алгоритма решения задачи

1) Провести кодирование исходного сообщения, преобразовав его в ASCII код. В пакете MathCAD данное преобразование осуществляется с помощью команды str2vec(s). При этом цифровое представление символов окажется в десятичной системе счисления.

2) Осуществить блочное шифрование полученного сообщения, с разбивкой его на блоки по 4 символа. В качестве алгоритмов шифрования используйте последовательно метод подстановки, метод перестановки. Ключ определяется индивидуально.

3) Сформировать дискретную последовательность данных зашифрованного сообщения. Преобразовать полученное закодированное зашифрованное сообщение в двоичный код, получив в конечном итоге последовательность битов.

4) Согласно индивидуальному заданию осуществить частотную (амплитудную) манипуляцию передаваемого сообщения. После манипуляции закодированный зашифрованный модулированный сигнал поступает в канал связи. После чего наступает этап получения информации.

5) Реализовать процедуру демодуляции/детектирования полученного сообщения. Согласно варианту проводимой модуляции, реализовать алгоритм демодуляции принимаемого сигнала.

6) Сформировать последовательность данных для дешифрования информации. Преобразовать закодированное сообщение в десятичный ASCII код. Отобразить зашифрованное сообщение.

7) Провести дешифрование полученного сообщения с помощью исходного ключа.

8) Провести декодирование сообщения.

Вывести исходный текст сообщения.

# 3 Практическая часть

Исходное сообщение «a snake lurks in the grass» нужно зашифровать с использованием блочного шифрования и методов подстановки и перестановки, далее осуществить перевод сообщения в двоичную последовательность и осуществить амплитудную манипуляцию. Эти шаги составляют этап отправления информации.

Далее следует этап получения информации на котором нужно провести демодуляцию сигнала, его дешифровку, декодирование и вывести полученный результат.

Все указанные действия проводились в пакете MathCAD.

# 3.1 Преобразование исходного сообщения в ASCII код

В пакете MathCAD преобразование в ASCII код осуществляется с помощью команды str2vec(s). При этом цифровое представление символов окажется в десятичной системе счисления. Открытый текст имеет длину 26 символов, по заданию нужно использовать блоки по 4 символа, для этого в конце передаваемого сообщение добавим два пробела.



# 3.2 Блочное шифрование.

Для блочного шифрования разобьем исходную последовательность разобьем на блоки по 4 символа и получим матрицу шифрования:



Далее воспользуемся алгоритмом замены (Шифр Цезаря) со смещением на k=5 и мощность алфавита n1=96:



Следующим применим алгоритм перестановки внутри каждого блока.

Для этого используем ключ: 

Преобразуем матрицу в вектор:



На выходе получим следующее зашифрованное сообщение:



Данное шифрование будет достаточно надежным, т.к. без знания ключа и сдвига дешифровка будет крайне затруднительна.

# 3.3 Амплитудная манипуляция

Предварительно преобразуем полученную в результате шифрования десятичную последовательность в последовательность двоичную:



Далее осуществляем амплитудную модуляцию. Кодирующие частоты –

ω=106, А1=16, А0=11.

 

 

В результате получаем сигнал, приведённый на рисунке 2.



Рисунок 2 – Модулированный сигнал

3.4 Демодуляция



# 3.5 Перевод двоичной системы в ASCII код



# 3.6 Дешифрование информации

Разобьем последовательность на блоки:



Далее наложим ключ:



Последним шагом дешифруем шифр Цезаря:



Преобразуем матрицу в вектор:



# 3.7 Результат

Получим сообщение:



Сообщение является исходным, поэтому передачу можно назвать успешной.

ЗАКЛЮЧЕНИЕ

По итогу, можно прийти к выводу, что использование нескольких алгоритмов шифрования при передаче сообщения может значительно повысить защищенность передаваемых данных. На практике же применение комбинирование алгоритмов шифрования, а именно шифра подстановки и шифра перестановки могут увеличить помехоустойчивость и защищенность сигналов, что является немаловажным, учитывая неоднородность условий передачи в реальном мире.

 Что касается модуляции, это не менее важный процесс, благодаря которому сигнал переносится в область высоких частот с целью увеличения количества передаваемых сигналов и дальности их передачи.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Маршаков Д.В. Обеспечение безопасного информационного обмена по незащищенному каналу связи: методические указания к курсовой работе, по дисциплине «Модели и методы безопасного информационного обмена». – Ростов на Дону: издательский центр ДГТУ, 2018г.
2. Прокис Дж. Цифровая связь. Пер. с англ. / Под ред. Д. Д. Кловского. — М.: Радио и связь, 2000.
3. Щербаков А.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических алгоритмов. – М.: Русская редакция, 2003. – 416 с.
4. Колотилов Ю.В., Кузнецов П.А., Лим В.Г. и др. Использование методов оценки информационного риска для выбора средств защиты информации в среде САПР на предприятиях строительного комплекса. - Вопросы защиты информации. – 2003. - № 3(62). - С.50-53.
5. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. – М.: ДМК Пресс, 2004. – 616 с.