Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Кафедра автоматизации и управления

КОМПЬЮТЕРНЫЕ СЕТИ В СИСТЕМАХ УПРАВЛЕНИЯ

Методические указания по выполнению расчетно-графических работ для студентов специальности 5В070200 – Автоматизация и управление

Алматы 2018

СОСТАВИТЕЛИ: Сябина Н.В., Ибраева Л.К. Компьютерные сети в системах управления. Методические указания по выполнению расчетно-графических работ для студентов специальности 5В070200 – Автоматизация и управление. - Алматы: АУЭС, 2018. – 24 с.

Для проверки знаний студентов, полученных в результате изучения тем для самостоятельной работы, в курсе «Компьютерные сети в системах управления» предусмотрены три расчетно-графические работы.

Настоящие методические указания предназначены в помощь студентам специальности 5В070200 – «Автоматизация и управление» и содержат варианты заданий, а также рекомендации по выполнению работ. Приложения содержат весь необходимый справочный материал.

Ил. 4, табл. 15, прилож. 3, библиогр. - 6 назв.

Рецензент: канд. техн. наук, доцент Мусапирова Г.Д.

Печатается по плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи» на 2018 г.

© НАО «Алматинский университет энергетики и связи», 2018 г.

1 Расчетно-графическая работа № 1. Проектирование локальной вычислительной сети организации

Цель: научиться принимать проектные решения с учетом специфики предприятия, выполнять расчет кабеля с учетом топологии сети.

1.1 Задание к расчетно-графической работе

1.1.1 В соответствии с выбранным вариантом задания (см. таблицу А.1) выполнить постановку задачи.

1.1.2 Разработать план помещений, указать размеры.

1.1.3 С учетом специфики организации выбрать топологию сети, технологии передачи данных, результаты отобразить на отдельном рисунке. Обосновать свой выбор.

1.1.4 Выбрать все необходимое оборудование; отобразить его размещение на плане. Обосновать выбор.

1.1.5 Выбрать кабель и указать на плане, как он будет проложен с учетом топологии. Выполнить расчет длины кабеля одним из известных методов. Обосновать свое решение.

1.1.6 Оформить отчет в соответствии с требованиями стандарта АУЭС.

1.2 Общие рекомендации к выполнению работы

Для определения структуры сети, взаимного расположения оборудования, выбора физической среды передачи данных, достаточно представления упрощённой схемы помещений с указанием их размеров.

Одним из первых шагов при планировании является выбор типа физической топологии сети. Как правило, исходят из четырех основных топологий – «шина», «звезда», «кольцо», «ячейка», каждая из которых имеет определенные недостатки. Поэтому на практике они редко встречаются в чистом виде, чаще используются гибридные топологии – «звезда на шине», «звезда на кольце» и т.п. При этом выбор базируется на множестве факторов таких, как расстояние, стоимость оборудования, предполагаемая сетевая операционная система, вопросы безопасности и т.п.

При выборе оборудования следует учитывать планируемую топологию сети, особенности помещений, предполагаемую сумму затрат, требования безопасности. Но при этом все решения необходимо тщательно обдумывать и обосновывать: дешевый вариант – не всегда лучший выбор и, если позволяет бюджет, выбор лучше сделать в пользу более функционального оборудования.

Неотъемлемой частью любой сети является кабель. В современных компьютерных сетях используются три типа кабеля: коаксиальный кабель (coaxial cable), витая пара (twisted pair) и оптоволоконный кабель (fiber optic). Типы кабеля отличаются друг от друга внутренним устройством и обладают рядом технических характеристик, влияющих на основные потребительские параметры сетей. При прокладке кабеля важно следовать стандартам,

разработанным для обеспечения определенного уровня производительности сети. Стандарты определяют типы кабелей, используемых в определенной среде, материалы проводников, схему расположения выводов, размеры проводов, экраны, длину кабелей, типы разъемов и предельные значения производительности.

При расчете количества кабеля для горизонтальной подсистемы существуют два основных метода вычисления:

- метод суммирования, который заключается в подсчете длины трассы каждого горизонтального кабеля с последующим сложением этих длин. К полученному результату добавляется технологический запас (до 10%), а также запас для выполнения кабельной разделки в розетках (0,6-1,0 м). Достоинством метода является высокая точность, но при отсутствии средств автоматизации и проектировании структурированной кабельной системы (СКС) с большим количеством портов этот подход оказывается слишком трудоемким;

- эмпирический метод заключается в том, чтобы применить эмпирическую формулу, которая поможет рассчитать общую горизонтальную кабельную длину, затрачиваемую для создания СКС. Применяется в случае, когда рабочих мест больше 30 и нужно рассчитать среднюю длину расхода витой пары. Формула выглядит следующим образом:

$$Lср = (Lмин + Lмакс) / 2 * 1.1 + X, \quad (1)$$

где *Lмин* и *Lмакс* – длины самой короткой и самой длинной кабельной линии;

X - запас для кабельной разделки (от 0,6 до 1,0 м).

Затем рассчитывается количество пробросов с одной упаковки кабеля по формуле:

$$N = Lкат / Lср, \quad (2)$$

где *Lкат* – длина кабеля в катушке (от 100 до 1000).

Полученное значение нужно округлить до целого минимального показателя. После чего подсчитывается количество портов и делится на количество пробросов в одной упаковке. Полученное значение округляется до большего из ближайших, а полученная цифра умножается на кабельную длину.

1.3 Контрольные вопросы

1.3.1 Что представляет собой физическая среда передачи данных?

1.3.2 Перечислите и охарактеризуйте известные способы коммутации.

1.3.3 Что понимается под топологией сети?

1.3.4 Перечислите базовые топологии. Каковы их особенности?

1.3.5 Какое устройство используется для физического соединения компьютера с сетью?

1.3.6 Какое устройство используется в качестве центральной точки соединения в сетевой конфигурации «звезда»? Какие устройства используются для соединения сетевых сегментов?

1.3.7 Что представляет собой СКС?

1.3.8 Перечислите характеристики разных типов кабелей.

1.3.9 В чем заключается метод суммирования?

1.3.10 В каком случае имеет смысл использовать эмпирический метод?

2 Расчетно-графическая работа № 2. Адресация компьютеров в Интернет

Цель: изучить способы адресации компьютеров в глобальной сети Интернет и алгоритмы вычисления основных характеристик по IP-адресу.

2.1 Задания к расчетно-графической работе

2.1.1 По указанному в таблице А.2 IP-адресу и маске определить класс сети и вычислить ее адрес. Используя методики, определить адрес рабочего хоста и количество рабочих узлов.

2.1.2 По указанному в таблице А.3 IP-адресу и сетевому префиксу определить класс сети, вычислить ее адрес, определить широковещательный адрес, адрес первого хоста, адрес последнего хоста, номер рабочего компьютера и количество доступных узлов.

2.1.3 Все переводы из одной системы счисления в другую выполнить вручную. Пояснить свои действия. Выполнить проверку с помощью IP Калькулятора подсетей http://infocisco.ru/ip_calculator.php.

2.1.4 Оформить отчет в соответствии с требованиями стандарта АУЭС.

2.2 Общие рекомендации к выполнению работы

IP-адрес определяет местонахождение узла в сети. Каждый IP-адрес состоит из двух частей - идентификатора сети и идентификатора узла. Идентификатор сети, который определяет физическую сеть, одинаков для всех узлов в одной сети и уникален для каждой из сетей, включенных в объединенную сеть. Идентификатор узла соответствует конкретной рабочей станции (серверу, маршрутизатору или другому TCP/IP-узлу в сети), имеет уникальное значение в данной сети.

IP-адрес может записываться в двух форматах - двоичном и десятичном. Каждый IP-адрес имеет длину 32 бита и состоит из четырех октетов (8-битных полей), которые отделяются друг от друга точками. Каждый октет представляет собой десятичное число в диапазоне от 0 до 255.

Для вычисления адреса сети можно воспользоваться следующим алгоритмом:

- перевести каждое из чисел в IP-адресе и маске в двоичную систему;

- выполнить поразрядную конъюнкцию IP-адреса компьютера в сети и его маски, перевести каждый октет в десятичную систему.

Для вычисления номера узла в сети применяется следующий алгоритм:

- перевести каждое из чисел в маске и IP-адресе в двоичную систему;
- отсчитать в маске сети количество нулевых бит;
- отсчитать в IP-адресе такое же количество последних бит и перевести это число в десятичную систему.

Сообществом Интернет определено пять классов IP-адресов в соответствии с различными размерами компьютерных сетей. Класс адреса определяет, какие биты относятся к идентификатору сети, а какие - к идентификатору узла. Кроме того, он определяет максимально возможное количество узлов в сети. Microsoft TCP/IP поддерживает классы A, B и C. Класс IP-адреса идентифицируют по значению его первого октета. В таблице 2.1 показывается, как определяются поля в IP-адресах разных классов. Значение 127 зарезервировано для диагностики и используется в качестве локальной заглушки, поэтому в качестве идентификатора сети не может использоваться.

Таблица 2.1 – Определение полей в IP-адресах

Класс	IP-адрес	Идентификатор сети	Идентификатор узла
A	W.X.Y.Z	W	X.Y.Z
B	W.X.Y.Z	W.X	Y.Z
C	W.X.Y.Z	W.X.Y	Z

Адреса класса A назначаются узлам очень большой сети. Старший бит в адресах этого класса всегда равен нулю. Следующие семь бит первого октета представляют идентификатор сети. Следующие три октета (24 бита) содержат идентификатор узла.

Адреса класса B назначаются узлам в больших и средних по размеру сетях. В двух старших битах IP-адреса класса B записывается двоичное значение 10. Следующие 14 бит (два первых октета) содержат идентификатор сети. Оставшиеся два октета (16 бит) указывают на идентификатор узла.

Адреса класса C применяются в небольших сетях. Три старших бита IP-адреса этого класса содержат двоичное значение 110. Следующие 21 бит составляет идентификатор сети (первые три октета). Оставшиеся 8 бит (последний октет) отводятся под идентификатор узла. Всего возможно около 2000000 сетей класса C, содержащих до 254 узлов.

Адреса класса D предназначены для рассылки групповых сообщений. Четыре старших бита в IP-адресе класса D всегда равны 1110. Оставшиеся биты обозначают вполне определенную группу получателей и не разделяются на части. Пакеты с такими адресами рассылаются избранной группе узлов в сети. Их получатели - только специальным образом зарегистрированные узлы. Microsoft поддерживает адреса класса D, которые применяются приложениями для групповой рассылки сообщений.

Класс E – экспериментальный и в настоящее время не применяется. Четыре старших бита адресов класса E равны 1111. Он зарезервирован для использования в будущем.

Класс сети можно определить по таблице Б.1.

2.3 Контрольные вопросы

2.3.1 Перечислите способы адресации компьютеров в Internet.

2.3.2 Что понимается под маской сети?

2.3.3 Что представляет собой IP-адрес?

2.3.4 Что такое сетевой префикс?

2.3.5 Какие классы сетей определены в соответствии с их размерами?

2.3.6 Как определить класс сети по IP-адресу?

2.3.7 С какой целью используется широковещательный адрес?

2.3.8 Что представляет собой доменная система имен?

2.3.9 Какие существуют способы настройки IP-адресов?

2.3.10 В чем отличие приватного и реального IP-адреса ?

3 Расчетно-графическая работа № 3. Защита информации в компьютерных сетях

Цель: изучить американский стандарт шифрования данных Data Encryption Standard (DES); получить практические навыки реализации фрагмента алгоритма шифрования и расшифрования данных.

3.1 Задания к расчетно-графической работе

3.1.1 Изучить алгоритм DES.

3.1.2 Выбрать исходный текст и ключ шифрования. Преобразовать исходный текст и ключ в двоичный код.

3.1.3 Ознакомиться с окном интерфейса алгоритма DES (программа *Project1_rus.exe*). Разместить двоичный код исходного текста и ключа в файлах *input code.txt* и *key.txt* в папке DES соответственно. Выполнить полный цикл шифрования и дешифрации в этом интерфейсе.

3.1.4 Программно реализовать преобразование заданного в варианте фрагмента (см. таблицу А.4).

3.1.5 Сравнить результаты, полученные в пп. 3.1.3, 3.1.4.

3.1.6 Оформить отчет в соответствии с требованиями стандарта АУЭС.

3.2 Общие рекомендации к выполнению работы

Алгоритм DES является очень трудоемким, поэтому в работе каждый студент реализует отдельный фрагмент алгоритма DES. Для проверки работы своего фрагмента алгоритма необходимы результаты выполнения

предшествующих шагов алгоритма и окончательный результат работы алгоритма - зашифрованный и, соответственно, расшифрованный тексты. Для выполнения расчетно-графической работы в качестве вспомогательного инструментария используется запускающий файл *Project1_rus.exe*, реализующей алгоритм DES. В главной форме этой программы, вводя исходный текст (двоичный) в соответствующее поле, можно получить промежуточные результаты и окончательный результат (шифртекст) реализации алгоритма DES. Также можно из шифрованного текста получить исходный.

3.2.1 Американский стандарт шифрования данных DES.

Стандарт DES предназначен для защиты от несанкционированного доступа к важной, но несекретной информации в государственных и коммерческих организациях США. Алгоритм использует комбинацию подстановок и перестановок. DES осуществляет шифрование 64-битовых блоков данных с помощью 64-битового ключа, в котором значащими являются 56 бит (остальные 8 бит - проверочные биты для контроля на четность). Расшифрование в DES является операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности. Обобщенная схема процесса шифрования в алгоритме DES показана на рисунке 3.1. Процесс шифрования заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах шифрования и, наконец, в конечной перестановке битов.

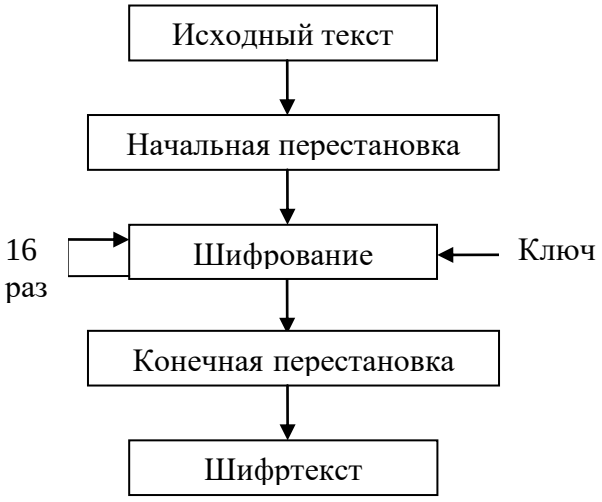

Рисунок 3.1 - Обобщенная схема шифрования в алгоритме DES

Все используемые в алгоритме таблицы являются стандартными и должны включаться в реализацию алгоритма DES в неизменном виде. Все перестановки и коды в таблицах подобраны разработчиками таким образом, чтобы максимально затруднить процесс расшифровки путем подбора ключа.

При описании алгоритма DES (рисунок 3.2) применены следующие обозначения:

L и R - последовательности битов (левая Left и правая Right);

LR - конкатенация последовательностей L и R, т.е. такая последовательность битов, длина которой равна сумме длин L и R; в последовательности LR биты последовательности R следуют за битами последовательности L;

«+» - операция побитового сложения по модулю 2.

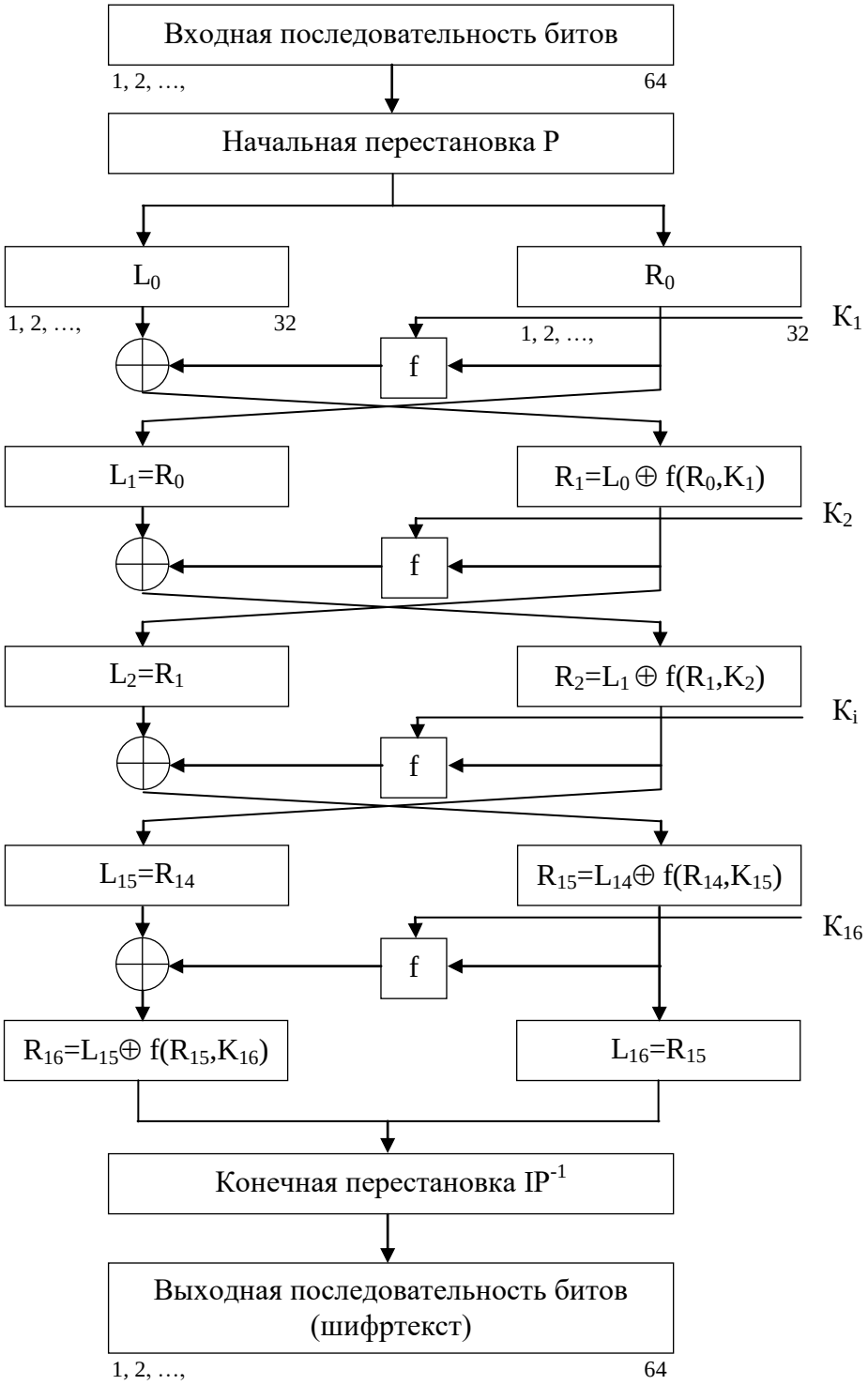

Рисунок 3.2 - Структура алгоритма DES

3.2.2 Описание алгоритма.

Пусть из файла исходного текста считан очередной 64-битовый (8-байтовый) блок T. Этот блок T преобразуется с помощью *матрицы начальной перестановки* IP (таблица В.1). Биты входного блока T (64 бита) переставляются в соответствии с матрицей IP: бит 58 входного блока T становится битом 1, бит 50 - битом 2 и т.д. Эту перестановку можно описать выражением $T_0 = IP(T)$. Полученная последовательность битов T_0 разделяется на две последовательности (L_0 - левые или старшие биты, R_0 - правые или младшие биты), каждая из которых содержит по 32 бита. Затем выполняется итеративный процесс шифрования, состоящий из 16 шагов (циклов). Пусть T_i - результат i-й итерации:

$$T_i = L_i R_i, \quad (3)$$

где $L_i = t_1, t_2, ..., t_{32}$ (первые 32 бита); $R_i = t_{33}, t_{34}, ..., t_{64}$ (последние 32 бита). Тогда результат i-й итерации описывается следующими формулами:

$$L_i = R_{i-1}, i = 1,2,...,16; \quad (4)$$

$$R_i = L_{i-1} + f(R_{i-1}, K_i), i = 1,2,...,16. \quad (5)$$

Функция f называется функцией шифрования. Ее аргументами являются последовательность R_{i-1}, получаемая на предыдущем шаге итерации, и 48-битовый ключ K_i, который является результатом преобразования 64-битового ключа шифра K.

На последнем шаге итерации получают последовательности R_{16} и L_{16} (без перестановки местами), которые конкатенируются в 64-битовую последовательность $R_{16}L_{16}$. По окончании шифрования осуществляется восстановление позиций битов с помощью матрицы обратной перестановки IP^{-1} (таблица В.2). Пример того, как соотносятся элементы первой строки матрицы IP^{-1} с элементами матрицы IP, приведен в таблице В.3.

Процесс расшифрования данных является инверсным по отношению к процессу шифрования. Все действия должны быть выполнены в обратном порядке. Это означает, что расшифровываемые данные сначала переставляются в соответствии с матрицей IP^{-1}, а затем над последовательностью битов $R_{16}L_{16}$ выполняются те же действия, что и в процессе шифрования, но в обратном порядке.

Итеративный процесс расшифрования может быть описан следующими формулами:

$$R_{i-1} = L_i, i = 1,2, ..., 16; L_{i-1} = R_i + f(L_i, K_i), i = 1,2.....16. \quad (6)$$

Таким образом, для процесса расшифрования с переставленным входным блоком $R_{16}L_{16}$ на первой итерации используется ключ K_{16}, на второй итерации - K_{15} и т.д. На 16-й итерации используется ключ K_1. На последнем шаге итерации будут получены последовательности L_0 и R_0, которые конкатенируются в 64-битовую последовательность L_0R_0. Затем в этой последовательности 64 бита переставляются в соответствии с матрицей IP. Результат преобразования - исходная последовательность битов (расшифрованное 64-битовое значение).

3.2.3 Вычисление функции шифрования.

Схема вычисления функции шифрования f (R_{i-1},K_i) показана на рисунке 3.3.

Для вычисления значения функции f используются:

- функция E (расширение 32 бит до 48);
- функция S_1, S_2, ..., S_8 (преобразование 6-битового числа в 4-битовое);
- функция P (перестановка битов в 32-битовой последовательности).

Приведем определения этих функций.

Аргументами функции шифрования f являются R_{i-1} (32 бита) и K_i (48 бит). Результат функции E (R_{i-1}) есть 48-битовое число. Функция расширения E, выполняющая расширение 32 бит до 48 (принимает блок из 32 бит и порождает блок из 48 бит), определяется таблицей В.4.

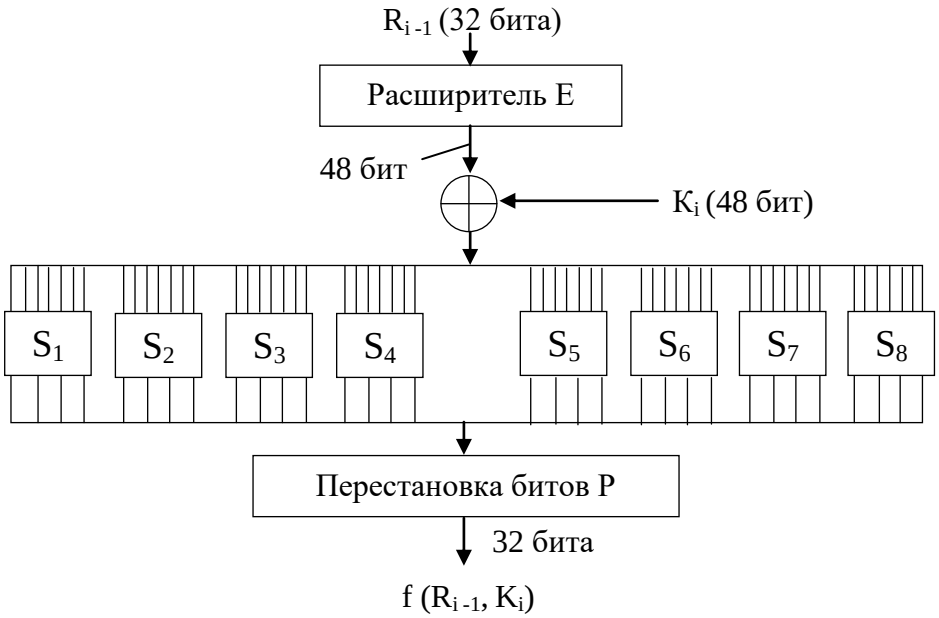

Рисунок 3.3 - Схема вычисления функции шифрования

В соответствии с таблицей 4 первые три бита E (R_{i-1}) - это биты 32, 1 и 2, а последние - 31, 32, 1. Полученный результат, E(R_{i-1}), складывается по модулю 2 (операция XOR) с текущим значением ключа K_i и затем разбивается на восемь 6-битовых блоков B_1, B_2, ... B_8:

$$E(R_{i-1}) + K_i = B_1\, B_2 ... B_8. \quad (7)$$

Далее каждый из этих блоков используется как номер элемента в функциях-матрицах S_1, S_2.....S_8, содержащих 4-битовые значения (таблица В.5).

Следует отметить, что выбор элемента в матрице S_i осуществляется достаточно оригинальным образом. Пусть на вход матрицы S_i поступает 6-битовый блок $B_j = b_1\, b_2\, b_3\, b_4\, b_5\, b_6$, тогда двухбитовое число $b_1\, b_6$ указывает номер строки матрицы, а четырехбитовое число $b_2\, b_3\, b_4\, b_6$ - номер столбца. Например, если на вход матрицы S_1 поступает 6-битовый блок $B_1 = b_1\, b_2\, b_3\, b_4\, b_5\, b_6 = = 100110$, то 2-битовое число $b_1\, b_6 = 10_{(2)} = 2_{10}$ указывает строку с номером 2 матрицы S_1, а 4-битовое число $b_2\, b_3\, b_4\, b_5 = 0011_{(2)} = 3_{(10)}$ указывает

столбец с номером 3 матрицы S_1. Это означает, что в матрице S_1 блок B_1 = 100110 выбирает элемент на пересечении строки с номером 2 и столбца с номером 3, т.е. элемент $8_{(10)}$ = $=1000_{(2)}$. Совокупность 6-битовых блоков B_1, B_2,..., B_8 обеспечивает выбор четырехбитового элемента в каждой из матриц S_1, S_2.....S_8.

В результате получаем $S_1(B_1)$ $S_2(B_2)$ $S_3(B_3)$ ... $S_8(B_8)$, т.е. 32-битовый блок (поскольку матрицы S_i содержат 4-битовые элементы). Этот 32-битовый блок преобразуется с помощью функции перестановки битов P (таблица В.6).

Таким образом, функция шифрования выглядит следующим образом:

$$f(R_{i-1}, K_i) = P(S_1(B_1).....S_8(B_8)). \quad (8)$$

3.2.4 Вычисление значения ключа.

Как нетрудно заметить, при вычислении функции шифрования на каждой итерации используется новое значение ключа K_j (длиной 48 бит). Новое значение ключа K_i вычисляется из начального ключа К (рисунок 3.4). Ключ К представляет собой 64-битовый блок с 8 битами контроля по четности, расположенными в позициях 8, 16, 24, 32, 40, 48, 56, 64. Для удаления контрольных битов и подготовки ключа к работе используется функция G первоначальной подготовки ключа (таблица В.7).

Таблица В.7 разделена на две части. Результат преобразования G(K) разбивается на две половины C_0 и D_0 по 28 бит каждая. Первые четыре строки матрицы G определяют, как выбираются биты последовательности C_0 (первым битом C_0 будет бит 57 ключа шифра, затем бит 49 и т.д., а последними битами - биты 44 и 36 ключа). Следующие четыре строки матрицы G определяют, как выбираются биты последовательности D_0 (т.е. последовательность D_0 будет состоять из битов 63, 55, 47, ...,12, 4 ключа шифра). Как видно из таблицы В.7, для генерации последовательностей C_0 и D_0 не используются биты 8, 16, 24, 32, 40, 48, 56 и 64 ключа шифра. Эти биты не влияют на шифрование и могут служить для других целей (например, для контроля по четности). Таким образом, в действительности ключ шифра является 56-битовым.

После определения C_0 и D_0 рекурсивно определяются C_i и D_i, i = 1, 2,...,16. Для этого применяются операции циклического сдвига влево на один или два бита в зависимости от номера шага итерации, как показано в таблице В.8. Операции сдвига выполняются для последовательностей C_i и D_i независимо. Например, последовательность C_3 получается посредством циклического сдвига влево на две позиции последовательности C_2, а последовательность D_3 - посредством сдвига влево на две позиции последовательности D_2, C_{16} и D_{16} получаются из C_{15} и D_{15} посредством сдвига влево на одну позицию.

Ключ K_i, определяемый на каждом шаге итерации, есть результат выбора конкретных битов из 56-битовой последовательности C_iD_i и их перестановки. Другими словами, ключ $K_i=H(C_iD_i)$, где функция H определяется матрицей, завершающей обработку ключа (таблица В.9).

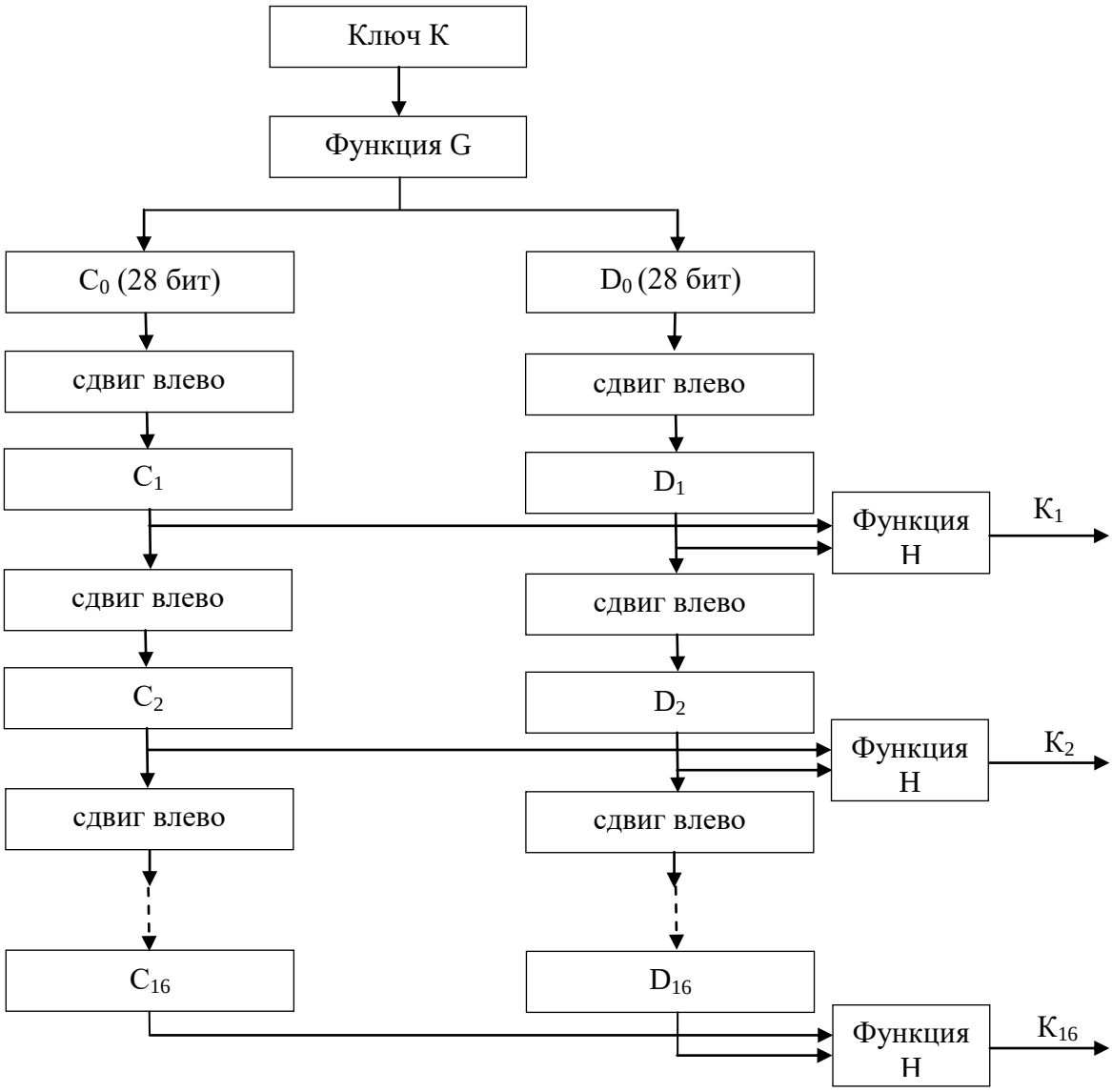

Рисунок 3.4 - Схема алгоритма вычисления ключей Kj

Как следует из таблицы В.9, первым битом ключа K_i будет 14-й бит последовательности C_iD_i вторым - 17-й бит, 47-м битом ключа K_i будет 29-й бит C_iD_i, а 48-м битом - 32-й бит C_iD_i.

3.3 Контрольные вопросы

3.3.1 Что понимается под информационной безопасностью сети?
3.3.2 Какими способами обеспечивается сетевая безопасность?
3.3.3 Перечислите этапы обеспечения безопасности предприятия.
3.3.4 Что представляет собой стандарт шифрования данных DES?
3.3.5 В чем заключается суть процесса шифрования?
3.3.6 Что представляет собой функция шифрования?
3.3.7 Перечислите аргументы функции шифрования f.
3.3.8 Что представляет собой ключ шифрования?
3.3.9 Как вычисляется ключ шифрования?
3.3.10 В чем заключается суть процесса расшифрования?

Приложение А

Варианты заданий

Таблица А.1 – Задание к расчетно-графической работе № 1

№ вар	Характеристика предприятия	Число помещений	Кол-во комп.	Особенности
1	Колледж, 3 факультета, 2 отдельно расположенных 3-х этажных корпуса.	5 – административных, 5 кафедр, 6 комп. классов, 15 лекционных аудиторий	10 10 60 15	Северный регион Казахстана. Корпуса находятся на расстоянии 200 м друг от друга, размеры 50х30, разделены парком.
2	Детский сад, 1 корпус, 3 этажа, отдельно стоящий домик охранника.	3 – административных, 2 – кухня, 1 – охранное, 10 – группы, 1 – актовый зал	10 1 1 5 2	Охранное помещение находится на расстоянии 150 м от главного входа в здание. Размер здания 40х30. Компьютеры в группах и на охране используются для записи с камер наблюдения.
3	Музей, 2-х этажное здание, длина 250 метров, подвальное помещение-хранилище, отдельно стоящий домик охранника.	2 – административных, 1 - охранное, 4 – хранилище, 8 выставочных залов	6 1 4 8	Охранное помещение находится на расстоянии 400 м от главного входа в здание, за парком. Компьютеры в залах, хранилище и на охране используются для записи с камер наблюдения.
4	Ресторанный комплекс, 3 здания 1-2-х этажных, расположенных на расстоянии друг от друга, отдельно стоящий домик охранника.	5 – административных, 3 – кухня, 2 – охранное, 8 – обеденные залы	12 3 4 8	Одно охранное помещение находится в главном здании, другое - на входе в комплекс, 200 м от главного здания. Часть компьютеров используется для записи с камер наблюдения. Размеры зданий – 20х20, 30х20, 20х20.
5	Школа, 4 этажа.	8 – административных, 2 – кухня, 1 – охранное, 5 комп. классов, 20 учебных классов	15 2 1 55 20	Охранное помещение находится на расстоянии 300 м от главного входа в здание. 1 компьютер в кухне и на охране используются для записи с камер наблюдения. Размеры здания - 50х30.

Продолжение таблицы А.1

№ вар	Характеристика предприятия	Число помещений	Кол-во комп.	Особенности
6	Кафе, 2-этажное здание.	5 – административных, 2 – кухня, 1 – охранное, 5 – обеденные залы	15 2 2 5	1 компьютер в кухне и на охране используются для записи с камер наблюдения. Размеры здания - 40х25.
7	Редакция газеты, 4-х этажное здание.	3 – административных, 15 – редакция, 2 - конференц-зал 1 – охранное, 2 - типография	10 75 10 2 10	Компьютер на охране используются для записи с камер наблюдения. Размеры здания - 40х25.
8	Спортивный комплекс, 3 отдельно стоящих 1-этажных здания.	5 – административных, 15 - спорт-залы, бассейн 3 – охранное, 2 – конференц-зал 10 – тренерская, 9 – для хранения инвентаря	20 15 6 4 20 9	Здания находятся на расстоянии 50 метров друг от друга, разделены игровыми площадками. Размеры зданий – 30х20, 40х20, 20х20. Охрана размещается в каждом из зданий. Раздевалки имеются по 2 в каждом из помещений для тренировок. Часть компьютеров используется для видеонаблюдения.
9	Развлекательный центр, размещенный на 2 этажах торгового центра.	2 – административных, 6 – игровые залы, 2- охранное	9 35 4	Размеры этажа – 50х40. Имеется зал компьютерных игр. Часть компьютеров используется для видеонаблюдения.
10	Туристическая компания, размещается на 3 этаже бизнес-центра.	1 - администрация, 1 - бухгалтерия, 1 - конференц-зал, 2 - агенты	7 5 1 10	Работа ведется на международном уровне, Требуется 24-часовой доступ к базам данных. Размеры этажа – 40х25.
11	Институт метеорологии и прогнозирования.	4 – административные, 20 – лаборатории, 6 - метеостанции	10 60 12	Институт – это 3-х этажное здание в центре города, размеры – 40х20. Метеостанции расположены за городской чертой

Продолжение таблицы А.1

№ вар	Характеристика предприятия	Число помещений	Кол-во комп.	Особенности
12	3-х этажный магазин крупной торговой сети.	3 - администрация, 1 - бухгалтерия, 3 – торговый зал, 2 - охранное	12 10 24 2	Охрана на каждом этаже. Размеры здания – 40х30. Часть компьютеров используется для видеонаблюдения.
13	Завод, 4 производственных корпуса и 2-х этажное административное здание.	14 – административных, 7 – цеха, 6 - охранное	40 15 5	Здания (50х40) находятся на расстоянии 300 метров друг от друга. Основные административные помещения находятся в адм. здании. 5 охранных помещений размещены в зданиях, 1 помещение – на проходной завода, в 400 м от административного здания.
14	Библиотека, помещения размещаются в 3 отдельных зданиях.	4 - администрация, 5 – читальный зал, 5 – абонемент, 1 – книгохранилище, 3 - охранное	10 60 10 4 3	Книгохранилище размещается в одном из зданий. Имеется 3 электронных читальных зала. 1 компьютер на абонементе предназначен для поиска по электронным каталогам. Часть компьютеров используется для видеонаблюдения. Размеры зданий – 20х20, 30х20, 20х20.
15	Магазин бытовой техники, одноэтажное здание.	3 – администрация, 1 – бухгалтерия, 4 – торговые залы, 2 – склады, 1 – торг.представители	7 5 8 4 2	Компьютер на охране используются для записи с камер наблюдения. Размеры здания - 40х25.
16	Научно-исследовательский центр, размещен на территории 2 кв. км, в 4 отдельно стоящих зданиях.	6 – администрация, 15 – лабораторий, 2 – испытательный полигон, 1 - охранное	8 90 10 2	Администрация размещается в отдельном здании (10х10). Испытательные полигоны размещены в одном здании (50х30). Размеры остальных зданий – 30х15. Охрана – на входе в центр.

Продолжение таблицы А.1

№ вар	Характеристика предприятия	Число помещений	Кол-во комп.	Особенности
17	Строительная компания, размещена в 3-х этажном здании.	10 – административные, 2 – офисы продаж, 4 – проектировщики, 12 – склады, 1 – охрана	15 6 20 12 1	Размеры здания – 30х20. Складские помещения – в подвальном помещении. Охрана размещается на въезде на территорию организации, в 50 метрах от входа, в отдельно стоящем помещении.
18	Больничный комплекс из трех 2-х этажных зданий на одной территории, с отдельно стоящим помещением охраны и аптекой.	3- административных, 2 - приемное отделение 1 – бухгалтерия, 5 – ординаторских, 5 - зав.отделением, 20 – лаборатории, 5 – реанимация, 2 - охрана, аптека	6 6 15 5 30 10 3	Охрана и аптека размещены на въезде на территорию больницы в 50 метрах от основного здания. Основное здание связано с двумя другими переходами по 30 м каждый. В обычных палатах компьютеры не установлены. Часть компьютеров используется для видео-наблюдения, для подключения к медицинскому оборудованию. Размеры зданий – 40х25.
19	Животноводческий комплекс.	2 – административные, 6 – животноводческие, 1 – лаборатория, 1 – ветеринарное, 1 - охрана	3 6 1 1 1	В животноводческих помещениях (30х10) компьютеры используются для наблюдения и обработки собранной информации с датчиков. Помещения размещены на расстоянии 50-1500 м друг от друга. Охрана размещена на въезде на территорию.
20	Телерадиокомпания, размещена в 4-х этажном здании.	6 – административные, 1 – бухгалтерия, 18 – рабочие помещения, 10 – редакции, 6 – студии, 2 – служба безопасности	10 5 40 50 20 5	Часть компьютеров используется для видеонаблюдения. Редакционные компьютеры – мобильные. Размер здания 50х20.

Таблица А.2 – Задание 1 к расчетно-графической работе № 2

№ варианта	IP-адрес	Маска
1	169.234.93.171	255.255.0.0
2	220.131.56.180	255.255.254.0
3	192.168.255.18	255.254.255.0
4	168.174.231.90	255.255.0.0
5	221.67.147.29	255.255.255.0
6	192.168.35.29	255.254.255.0
7	172.18.165.30	255.254.0.0
8	169.156.116.161	255.255.0.0
9	192.251.38.183	255.255.255.0
10	172.30.109.15	255.254.0.0
11	192.168.135.16	255.255.255.0
12	180.167.23.81	255.255.0.0
13	196.84.156.35	255.255.255.0
14	172.27.115.35	255.255.0.0
15	192.211.131.24	255.255.255.0
16	190.235.41.135	255.255.0.0
17	218.235.147.29	255.255.254.0
18	135.147.15.29	255.255.0.0
19	164.168.20.117	255.255.0.0
20	182.216.115.46	255.255.0.0

Таблица А.3 – Задание 2 к расчетно-графической работе № 2

№ варианта	IP-адрес	Сетевой префикс
1	220.126.15.131	/5
2	172.168.13.21	/19
3	147.21.135.215	/21
4	192.225.220.17	/4
5	128.38.124.51	/17
6	134.129.15.41	/13
7	198.44.215.21	/7
8	220.145.17.211	/4
9	154.168.27.116	/14
10	194.214.56.71	/6
11	136.81.216.31	/22
12	196.68.145.62	/8
13	154.82.157.13	/18
14	192.85.113.53	/3
15	168.34.251.18	/12
16	198.31.246.117	/5
17	168.24.156.21	/15
18	192.33.156.37	/4
19	221.15.31.79	/7
20	220.54.133.78	/8

Таблица А.4 – Задание к расчетно-графической работе № 3

№ варианта	Задание	Используемые элементы
1	Реализация алгоритма шифрования	
1.1	Сформировать из исходного текста 64-битовую последовательность T.	
1.2	Преобразовать блок T с помощью матрицы начальной перестановки IP и получить последовательность T_o = IP(T).	Таблица 1
1.3	Реализовать процесс шифрования: $L_I = R_{I-1}$, i = 1,2.....16; $R_i = L_{i-1} + f(R_{i-1}, Ki)$, i= 1,2.....16.	п/п-ы функции шифрования и вычисления ключа
2	Реализация алгоритма расшифрования	
2.1	Восстановить позиции битов с помощью матрицы обратной перестановки IP^{-1}	Таблица 2
2.2	Реализовать итеративный процесс расшифрования: $R_{i-1} = Li$, i = 1,2, ..., 16; $L_{i-1} = R_i + f(L_i, K_i)$, i = 1,2.....16	п/п-ы функции шифрования и вычисления ключа
3	Реализация функции шифрования $f(R_{i-1}, Ki)$	
3.1	Реализация функции расширения E	Таблица 4
3.2	Реализация функций S_1, S_2, ..., S_8 (преобразование 6-битового числа в 4-битовое)	Таблица 5
3.3	Реализация функции P (перестановка битов в 32-битовой последовательности	Таблица 6
4	Преобразование ключа K_j	
4.1	Реализация функции G первоначальной подготовки ключа	Таблица 7
4.2	Рекурсивное определение C_i и D_i, i = 1, 2.....16.	Таблица 8
4.3	Реализация функции H, завершающей обработку ключа	Таблица 9
5	Объединение всех блоков в одну программу	

Приложение Б

Адресация в сети Интернет

Таблица Б.1 - Классы IP-адресов

Класс	Диапазон значений первого октета	Первые биты первого октета	Сетевые/хостовые октеты (N=сеть, H=хост)	Маска подсети по умолчанию	Количество сетей	Хостов в каждой подсети (возможные к использованию адреса)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 (2^7 – 2)	16,777,214 (2^{24} – 2)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 (2^{14} – 2)	65,534 (2^{16} – 2)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 (2^{21} – 2)	254 (2^8 – 2)
D	224 – 239	1110	Зарезервировано для мультикастинга			
E	240 – 254	1111	Зарезервировано, используется для исследований			

Приложение В

Стандартные таблицы, используемые в алгоритме DES

Таблица В.1- Матрица начальной перестановки IP

58	50	42	34	26	48	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Таблица В.2 - Матрица обратной перестановки IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Таблица В.3 - Связь элементов матриц

Элемент матрицы IP^{-1}	Элемент матрицы IP
40	01
8	02
48	03
16	04
56	05
…	…

Таблица В.4 - Функция расширения E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Таблица В.5 - Функции преобразования S_1, S_2, ... , S_8

		Номер столбца																
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Номер строки	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	13
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
	2	4	1	4	8	13	6	2	11	15	12	9	7	3	10	5	0	
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	1	6	
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Таблица В.6 - Функция P перестановки битов

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Таблица В.7 - Функция G первоначальной подготовки ключа (переставленная выборка1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Таблица В.8 - Таблица сдвигов s_i для вычисления ключа

Номер итерации	Количество s_i сдвигов влево, бит	Номер итерации	Количество s_i сдвигов вправо, бит
1	1	9	1
2	1	10	2
3	2	11	2
4	2	12	2
5	2	13	2
6	2	14	2
7	2	15	2
8	2	16	1

Таблица В.9 - Функция H завершающей обработки ключа (переставленная выборка 2)

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Список литературы

1 Новиков Ю.В. Основы локальных сетей. - М.: «Бином», 2014.

2 Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. – М., 2014.

3 Горнец Н.Н. ЭВМ и периферийные устройства. Компьютеры и вычислительные системы. – М.: «Академия», 2012.

4 Малюк А.А. Введение в защиту информации в автоматизированных системах – М., 2011.

5 Бройдо В.Л. Вычислительные системы, сети и телекоммуникации. – СПб.: «Питер», 2008.

6 Олифер В.Г. Сетевые операционные системы. - СПб., 2008.

Содержание

1 Расчетно-графическая работа № 1. Проектирование локальной вычислительной сети организации 3
2 Расчетно-графическая работа № 2. Адресация компьютеров в Интернет 5
3 Расчетно-графическая работа № 3. Защита информации в компьютерных сетях 7
4 Приложение А 14
5 Приложение Б 20
6 Приложение В 21
Список литературы 24