Лабораторная работа №5. Реализация шифра *DES*

Цель работы: создать криптографическую систему шифрования данных, которая базируется на алгоритме шифровании *DES*. Алгоритм *DES* является первым симметричным алгоритмом блочного шифрования данных.

Теоретическая часть

Основные этапы алгоритма *DES* при шифровании текста:

1. Генерируется (задается) случайная последовательность Q из 56 бит.

2. В последовательность Q, для контроля четности, добавляются восемь контрольных битов в позиции

$$8, 16, 24, \ldots, 64.$$

Получается блок U размером в 64 бита.

3. Для удаления контрольных битов из блока U и формирования ключа K для шифрования, блок U преобразуют, используя функцию $G(U)$. Функция G определяется в виде стандартной таблицы, которую надо использовать в неизменном виде. В результате преобразования получают блок

$$K=G(U),$$

размером в 56 бит. Блок K разбивают на две половины $C0$ и $D0$ по 28 бит.

4. Используя $C0$ и $D0$, последовательно определяются Ci и Di , i = 1, 2, …, 16. Для формирования Ci и Di применяют операции циклического сдвига влево на один или два бита. Величина сдвига определяется стандартной таблицей. Операции сдвига для Ci и Di выполняются независимо. Последовательность $C5$ получается из $C4$ посредством циклического сдвига влево на 2 бита, а $D5$ – посредством циклического сдвига влево на 2 бита $D4$ (см. таблицу сдвигов для вычисления ключа на рисунке 5). В результате четвертого этапа формируется 16 ключей для 16 раундов алгоритма *DES*.

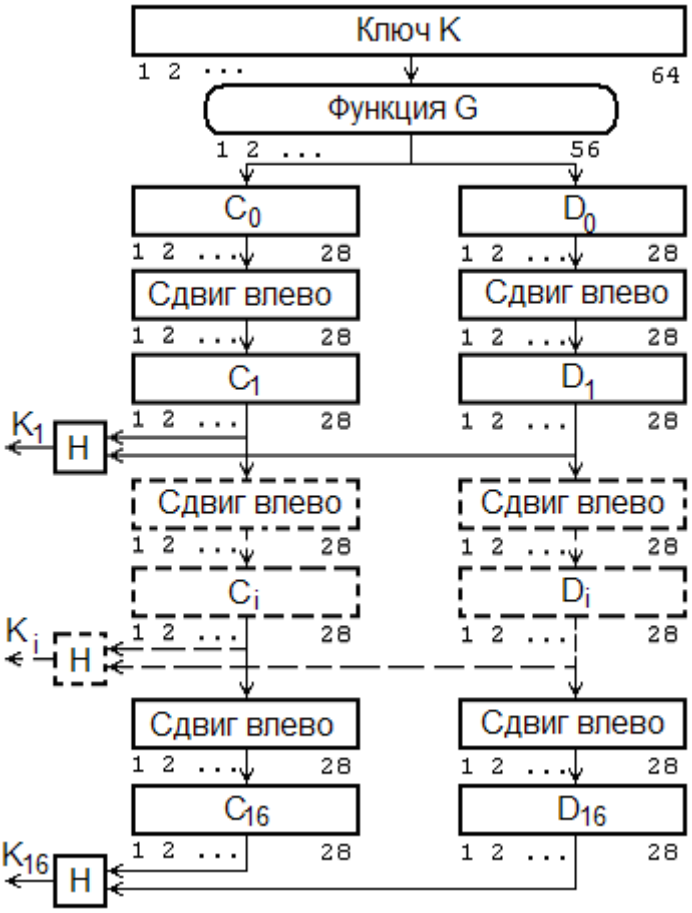

Рисунок 5 – Таблица сдвигов для вычисления ключа

5. Завершающий этап формирования ключей. Используя перестановку *H*, которая задается стандартной таблицей, каждый ключ размером в 56 бит преобразуется в блок из 48 бит. Данным преобразованием завершается этап формирования ключей.

6. Текущий блок открытого текста размером в 64 бит, представленный в виде двух 32 битовых блоков (*L*0*R*0) преобразуется начальной перестановкой *IP*, которая задается фиксированной стандартной таблицей.

7. Выполняется 16 раундов преобразований по следующим формулам

$$Li = Ri\text{-}1,$$

$$Ri = Li\_\oplus f(Ri\text{-}1, Ki),$$

$$i = 1.2, \ldots, 16.$$

Функция $f(Ri\text{-}1, Ki)$ представляет собой некоторую суперпозицию простых преобразований, детальное описание которых будет дано ниже. Отметим, что функция $f(Ri\text{-}1, Ki)$ является нелинейной. Нелинейность функции $f(Ri\text{-}1, Ki)$ обеспечивается S-блоками.

Алгоритм вычисления функции шифрования $f(Ri\text{-}1, Ki)$

К блоку $Ri\text{-}1$ применяют функцию расширения $E(Ri\text{-}1)$, которая 32-битовый блок $Ri\text{-}1$ преобразовывает в блок $R\prime = E(Ri\text{-}1)$ размером в 48 бит. Функция $E(Ri\text{-}1)$ определяется стандартной таблицей. Алгоритм вычисления функции шифрования формулируется следующим образом.

• Вычисляется новый блок размером в 48 бит по формуле

$$B = E(Ri\text{-}1) \oplus Ki.$$

• Блок B размером в 48 бит разбивается на восемь блоков Bj, j=1,2,…, 8, по шесть битов каждый

$$B = B1B2B3B4B5B6B7B8.$$

• Каждый блок Bj размером в шесть бит, используя свою функцию Sj , преобразуется в блок $Sj(Bj)$ размером в четыре бита. В результате получается следующий блок данных

$$B' = S1(B1)\ S2(B2)\ S3(B3)\ S4(B4)\ S5(B5)\ S6(B6)\ S7(B7)\ S8(B8)$$

размером в 32 бита.

• Алгоритм преобразования блока Bj размером в шесть бит в блок $Sj(Bj)$ размером в четыре бита следующий. Каждая функция Sj представляет собой стандартную таблицу, которая состоит из четырех строк с номерами 0, 1, 2, 3, и шестнадцати столбцов с номерами 0,1,2,…,15. Пусть, например, некоторый блок

$$Bj = b1\ b2\ b3\ b4\ b5\ b6 = 110010,$$

$$j = 1, 2, \ldots, 8.$$

Тогда имеет место:

биты $b1b6 = 10$ формируют номер столбца (двоичное число 10 равно десятичному числу 2) таблицы Sj,

биты $b2\ b3\ b4\ b5 = 1001$ формируют номер строки (двоичное число 1001 равно десятичному числу 9) таблицы Sj. Блок $Bj = b1\ b2\ b3\ b4\ b5\ b6 = 110010$ заменяют двоичным значением числа таблицы Sj, которое находится на пересечение строки с номером $b1b6 = 10$ (2) со столбцом с номером $b2\ b3\ b4\ b5 = 1001$ (9). Преобразуя каждое Bj,

Задание к работе

Программная реализация криптографической системы, основанной на алгоритме шифрования *DES*, должна быть оформлена как некоторая программная оболочка. В программной реализации должен быть разработан интерфейс, удобный для эксплуатации программы, в интерфейсе следует предусмотреть:

• два режима формирования ключа – ключ задан, ключ формируется по умолчанию;

• ввод начальной информации из сформированного заранее файла и из файла, который создается в оболочке программы;

• режимы шифрования, которые предусмотрены в *DES*;

• режимы шифрования и дешифрования информации.

Подготовить отчет по работе. В отчете описать алгоритм *DES*, описать структуру представления данных в программе, основные функции программы, назначение функций, входные и выходные параметры функций.

В отчет включить описание алгоритма генерации ключа, детали программной реализации, которые представляют интерес с точки зрения разработчика.