Лабораторная работа № 3
АЛГОРИТМ ШИФРОВАНИЯ ДАННЫХ DES

Цель работы

Познакомиться с основами симметричного шифрования. Изучить алгоритм шифрования DES на примере упрощенной версии S-DES.

Методические указания

1. Описание алгоритмов шифрования и расшифрования S-DES.

Среди современных методов традиционного шифрования долгое время самым распространённым являлся алгоритм DES (Data Encryption Standard). В 1977 году DES был утверждён и получил официальное имя: Federal Information Processing Standard 46 (FIPS PUB 46).

Алгоритм DES относится к группе симметричных алгоритмов, называемых сетями Файстеля.

Упрощенный S-DES – это алгоритм шифрования по структуре подобный DES, но имеющий меньше параметров. S-DES был разработан профессором Эдвардом Шейфером в учебных целях.

S-DES получает на входе 8-битовый блок открытого текста и 10-битовый ключ. В результате получается 8-битовый блок шифрованного текста. Используется 2 раунда шифрования.

Общая структура алгоритма шифрования S-DES представлена на рисунке 1.

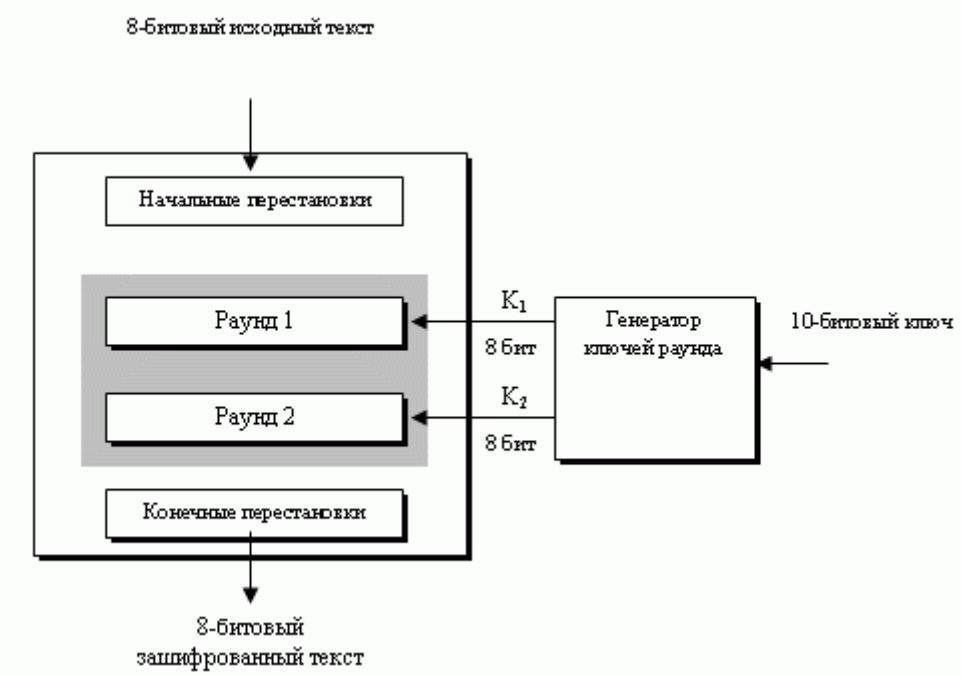

Рисунок 1 – Общая структура S-DES

Алгоритм шифрования S-DES включает в себя последовательное выполнение 5-ти операций:

- начальная перестановка (IP);
- функция f_k — является композицией операций перестановки и подстановки, зависит от подключа раунда;
- перестановка SW ;
- f_k ;
- IP^{-1} - перестановка, обратная начальной.

Расшифрование производится по той же схеме, только подключи раундов подаются в обратном порядке.

2. Вычисление подключей S-DES.

В S-DES используется 10-битовый ключ, который должен быть как у отправителя, так и у получателя сообщения. Из этого ключа генерируются два 8-битовых подключа.

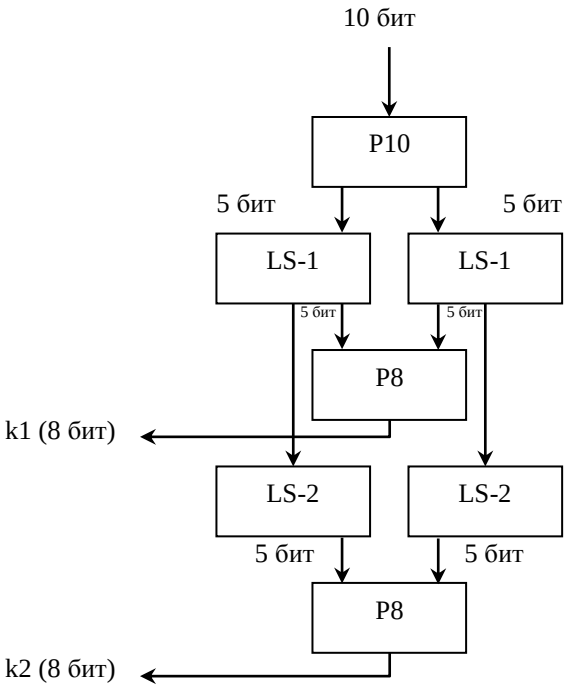

Рисунок 2 – Вычисление подключей раундов

Пример. Пусть имеем на входе следующий ключ $K=642_{(10)}$:

$$K=\begin{Bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ k_1 & k_2 & k_3 & k_4 & k_5 & k_6 & k_7 & k_8 & k_9 & k_{10} \end{Bmatrix}$$

1) Перестановка P10.

$$K=\begin{Bmatrix} 3 & 5 & 2 & 7 & 4 & 10 & 1 & 9 & 8 & 6 \\ k_3 & k_5 & k_2 & k_7 & k_4 & k_{10} & k_1 & k_9 & k_8 & k_6 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{Bmatrix} \quad (P10)$$

2) Циклический сдвиг влево на одну позицию. Выполняется отдельно для первых 5-ти битов и отдельно для вторых 5-ти битов.

$$K=\begin{Bmatrix} 5 & 2 & 7 & 4 & 3 & 1 & 9 & 8 & 6 & 10 \\ k_5 & k_2 & k_7 & k_4 & k_3 & k_1 & k_9 & k_8 & k_6 & k_{10} \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{Bmatrix}$$

3) Перестановка P8.

$$K=\begin{Bmatrix} 6 & 3 & 7 & 4 & 8 & 5 & 10 & 9 & - & - \\ k_1 & k_7 & k_9 & k_4 & k_8 & k_3 & k_{10} & k_6 & - & - \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & - & - \end{Bmatrix} \quad (P8)$$

Получаем первый 8-битный подключ $k_1 = 10100100$.

4) Циклический сдвиг влево на две позиции.

$$K=\begin{Bmatrix} 7 & 4 & 3 & 5 & 2 & 8 & 6 & 10 & 1 & 9 \\ k_7 & k_4 & k_3 & k_5 & k_2 & k_8 & k_6 & k_{10} & k_1 & k_9 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{Bmatrix}$$

5) Перестановка P8.

$$K=\begin{Bmatrix} 6 & 3 & 7 & 4 & 8 & 5 & 10 & 9 & - & - \\ k_8 & k_3 & k_6 & k_5 & k_{10} & k_2 & k_9 & k_1 & - & - \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & - & - \end{Bmatrix} \quad (P8)$$

Получаем второй 8-битный подключ $k_2 = 01000011$.

Т.о. получено два подключа, в каждом из которых выделим правую и левую части:

$k_1 = 1010|0100$

$k_2 = 0100|0011$

3. Алгоритм шифрования.

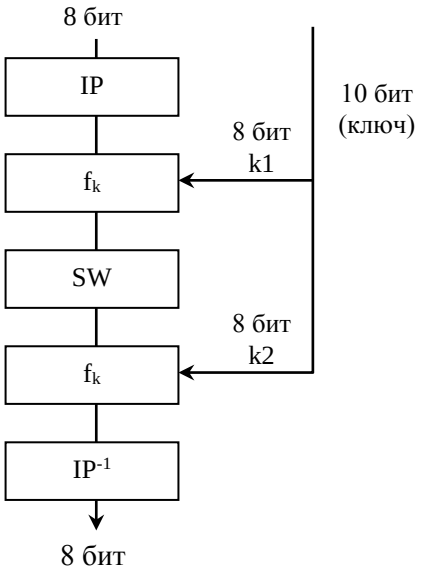

Рисунок 3 - Алгоритм шифрования S-DES

Начальная и конечная перестановки IP и IP^{-1} представлены на рисунке 4.

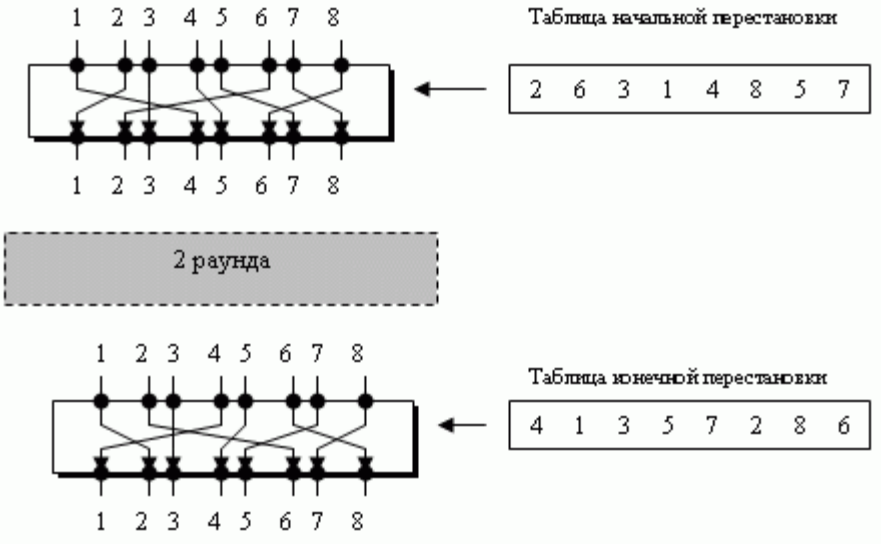

Рисунок 4 - Начальная и конечная перестановки IP и IP^{-1}

Операция 1: Начальная перестановка $IP: \{2 \quad 6 \quad 3 \quad 1 \quad 4 \quad 8 \quad 5 \quad 7\}$.
Пусть шифруемый символ $"t" = 116_{10} = 01110100_2$, $L = 0111, R = 0100$), тогда
$IP = 11101000, L = 1110, R = 1000$.

Операции 2: Функция f_k. представляет собой комбинацию перестановки и подстановки:

$$f_k.(L, R) = (L \oplus F(R, SK), R),$$

где L и R – левые и правые 4 бита 8-битовой последовательности, подаваемой на вход f_k.;
SK – подключ.

Отображение F.

На входе отображения имеем 4-битовое значение.

а) Сначала выполняется E/P — операция расширения/перестановки: $E/P = 41232341$, применяется к правой части;

для примера имеем: *E/P (R)* = 01000001;

$k_1 = 1010|0100$

б) $XOR(E/P, k_1) = 11100101, L = 1110, R = 0101$;

в) применение S-матриц:

$$S_L = \begin{matrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 1 \end{matrix}, \; S_R = \begin{matrix} 1 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{matrix}.$$

S-матрицы работают следующим образом: 1-ый и 4-ый биты входной последовательности рассматриваются как двухбитовые числа, определяющие строку S-матрицы, 2-ой и 3-ий биты — как числа,

определяющие столбец S-матрицы. Элементы, находящиеся на пересечении строки и столбца, задают двухбитовые выходные значения:

$L = 1|11|0$ *oper* $S_L = S_L[\,10_2, 11_2] = S_L[\,2_{10}, 3_{10}] = 3_{10} = 11_2$;
$R = 0|10|1$ *oper* $S_R = S_R[\,01_2, 10_2] = S_R[\,1_{10}, 2_{10}] = 1_{10} = 01_2$;
Получаем 4-битовую последовательность: 1101;

г) Перестановка $P4 = 2431$ даёт на выходе: $P4(1101) = 1101$.
е) $XOR(L, P4) = 1110\ XOR\ 1101 = 0011$.

Операция 3: *SW* – перестановка, меняет местами первые и последние 4 бита:
$SW(0011, R) = R|0011 = 1000|0011$
.

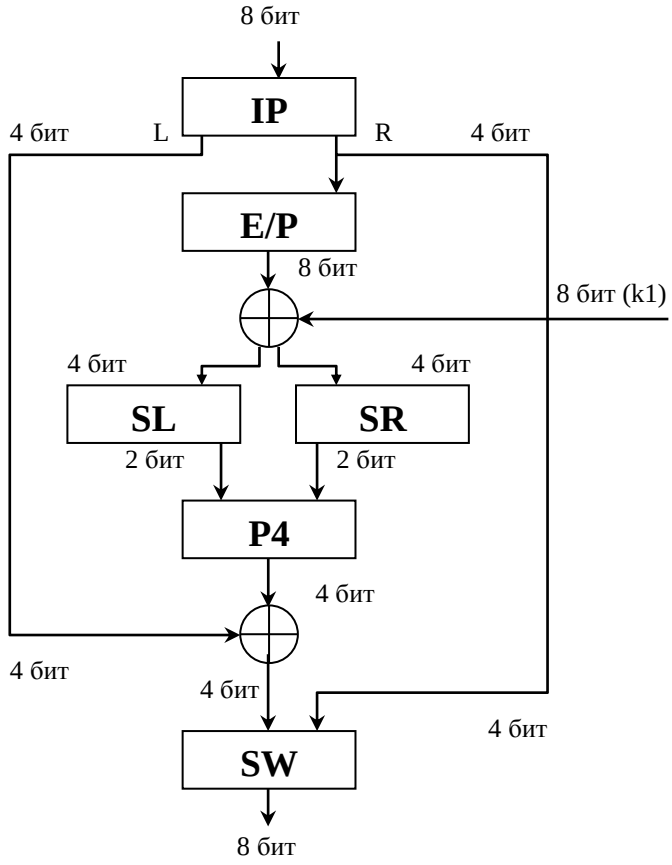

Схема f_k (операции 2, 4)

Операция 4: Функция f_k. К полученной последовательности битов применяем операцию 2, с той лишь разницей, что используется подключ k_2.

Операция 5: Завершающая перестановка. Является обратной по отношению к начальной.

$$IP^{-1}: \{4\quad 1\quad 3\quad 5\quad 7\quad 2\quad 8\quad 6\}$$

На выходе получим 8-битовый блок, который затем преобразуем в символ, который и будет являться зашифрованным.

Для расшифрования используется тот же алгоритм, что и для шифрования, только в операции 2 используется подключ k_2, а в операции 4 — подключ k_1.

Задания на лабораторную работу

1. Изучить основы симметричного шифрования
2. Изучить алгоритмы шифрования DES и S-DES.
3. Написать программы шифрования и расшифрования одного символа с использованием алгоритма S-DES.

При шифровании/расшифровании ключ и символ вводить с клавиатуры в двоичном или десятичном виде (как значение ASCII-кода символа). Промежуточные значения выводить на экран в двоичном виде. Результат шифрования/расшифрования выводить на экран в двоичном или десятичном виде.

Содержание отчета по лабораторной работе

1. Цель работы.
2. Описание программы.
3. Текст программы.
4. Результаты работы программы.
5. Выводы.

Контрольные вопросы

1. Какие преобразования называются несингулярными? Приведите пример сингулярного и несингулярного преобразований.
2. Какова структура сети Файстеля?
3. Какая сеть Файстеля называется классической? Гомогенной?
4. Как выполняется расшифрование в сетях Файстеля?
5. От чего зависит криптоаналитическая стойкость шифра Файстеля?
6. Классифицируйте алгоритм DES. Является ли он сетью Файстеля? Почему?
7. Проведите сравнение алгоритмов DES и S-DES по основным параметрам (длина ключа, длина блока шифрования, количество раундов, количество подключей, размер и количество S-блоков).
8. Являются ли криптостойким алгоритм DES? Можно ли его применять на практике? Обоснуйте ответ.
9. Какие типы операций используются в большинстве современных блочных алгоритмах симметричного шифрования?