Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет инфокоммуникаций
Кафедра защиты информации

Тема работы:

DES В РЕЖИМЕ РАСШИФРОВАНИЯ ШИФРТЕКСТОВ

Вариант №17

Студент: Савич О.А, Савченко Е.А
Номер группы: 961401
Преподаватель: А.М. Тимофеев

Минск 2022

Цель: изучение схемы расшифрования шифртекстов DES.

Краткие теоретические сведения.

Структурная схема алгоритма DES в режиме расшифрования шифртекстов приведена на рисунке 1.

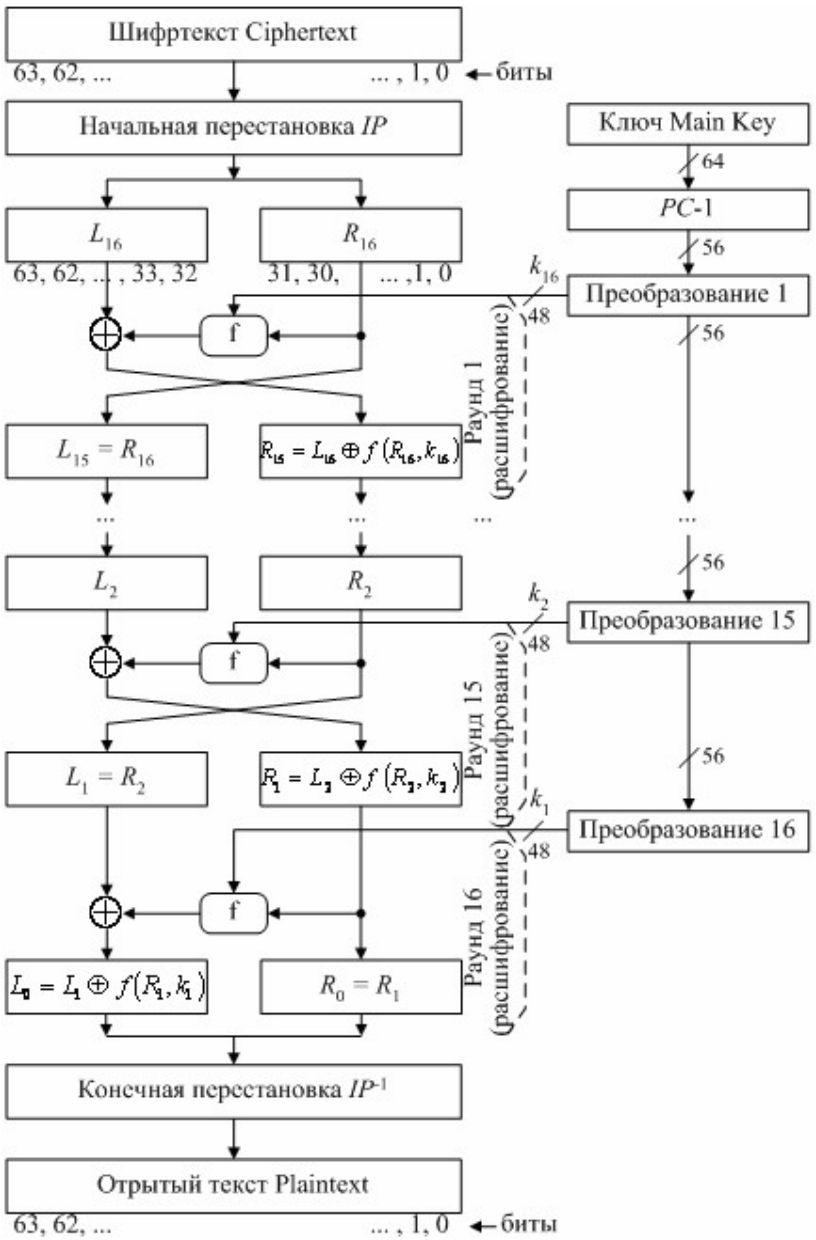

Рисунок 1 - Структурная схема алгоритма DES в режиме расшифрования шифртекстов

По сравнению со схемой зашифрования данных, алгоритм DES в режиме расшифрования шифртекстов является инверсным. С учетом логики работы алгоритма DES это означает, что расшифровываемые данные (биты шифртекста Ciphertext) сначала переставляются в соответствии с матрицей начальной перестановки *IP*, а затем над полученной последовательностью битов $R_{16}L_{16}$ выполняются те же действия, что и в процессе зашифрования данных над последовательностью R_0L_0 при зашифровании данных.

Таким образом, итеративный процесс расшифрования шифртекстов DES может быть описан следующими системами:

$$\begin{cases} L_{i-1} = R_i \\ R_{i-1} = L_i \oplus f(R_i, k_i) \end{cases}, i = 16,15,\ldots,2;$$
$$\begin{cases} L_0 = L_1 \oplus f(R_1, k_1) \\ R_0 = R_1 \end{cases} \quad (1)$$

Как видно из рисунка 1, на первой итерации используется раундовый ключ k_{16}, на второй итерации - k_{15} и т.д, а на шестнадцатой итерации - k_1.

На последнем шаге итерации получают последовательности R_0 и L_0 (без перестановки местами), которые конкатенируются в 64-битовую последовательность R_0L_0.

По окончании расшифрования осуществляется восстановление позиций битов с помощью матрицы конечной перестановки IP^{-1}, в результате чего формируются биты отрытого текста Plaintext (см. рисунок 1).

Полученные результаты практических расчетов:

– $L_{16}R_{16}$ = 44B4440B6AEDD112;

– $L_{15}R_{15}$ = 6AEDD112675FDBB2;

– $L_{14}R_{14}$ = 675FDBB2803C1401;

– $L_{13}R_{13}$ = 803C140169EDAB2F;

результаты, полученные средствами автогенерации учебного модуля:

– $L_{12}R_{12}$ = 69EDAB2F184D63E6;

– $L_{11}R_{11}$ = 184D63E6002155D3;

– $L_{10}R_{10}$ = 002155D30C8CBCA1;

– L_9R_9 = 0C8CBCA13C6B653D;

– L_8R_8 = 3C6B653D899FFE10;

– L_7R_7 = 899FFE104D8B9F99;

– L_6R_6 = 4D8B9F999D2A4328;

– L_5R_5 = 9D2A43285F11FEDF;

– L_4R_4 = 5F11FEDFDE7B8ECF;

– L_3R_3 = DE7B8ECFD6282336;

– L_2R_2 = D6282336A1B3B6D4;

– L_1R_1 = A1B3B6D4BB7DEBDC;

– L_0R_0 = 36BBF904BB7DEBDC;

– отрытый текст Plaintext = BCD863BEF6FC2E9E.

Контрольные вопросы:

1 В чем отличия работы схемы расшифрования шифртекстов от схемы шифрования данных DES?

Использование ключей в обратном порядке, расшифрование начинается с L16R16

2 Могут ли быть видоизменены таблицы (матрицы) E, S и P, а также таблицы (матрицы) начальной и конечной перестановки при реализации схемы

расшифрования шифртекстов DES для повышения информационной безопасности криптосистемы? Если да, то каким образом? Если нет, то почему?

E, S, P не могут быть изменены, потому что при разработке стандарта была выведена определенная криптостойкость, которая при данном условии упадет.

Таблицы (матрицы) начальной и конечной перестановки являются взаимообратными, следовательно, они могут быть изменены.

3 Какова вычислительная сложность реализации схемы расшифрования шифртекстов DES для современных аппаратно-программных средств?

Чем больше количество блоков, тем выше вычислительная сложность. При условии блока длиной 64 бита и использовании современных вычислительных средств, данная задача не будет относиться к сложным.

4 Можно ли использовать алгоритм DES для аутентификации данных, принятых из канала связи? Если да, то каким образом? Если нет, то почему?

Да, можно. Для реализации необходимо использовать режим сцепления блоков шифртекста, режим обратной связи по шифртексту.

5 В чем заключается сущность реализации алгоритма Triple DES? Каким образом при этом осуществляется расшифрование шифртекстов?

Длина ключа DES- 56 бит, 112 бит – 2DES, 168 бит – 3DES.

DES(k3; DES(k2; DES(k1; M))).

k1, k2, k3 – ключи для каждого шага.

Повышается криптостойкость, но уменьшается скорость работы.

Выводы по результатам выполнения работы:

В ходе выполнения данной лабораторной работы была изучена и выполнена схема расшифрования данных в соответствии со стандартом DES. Выполнено три итерации функции расшифрования, состоящих из функции расширения E, преобразования S, и перестановки P.

Отчет сформирован (не удалять!!! не изменять!!!):

1 Дата и время: 08.12.2022 18:13;

2 Вариант №: 17;

3 Студент: Савич Савченко;

4 Номер группы: 961401;

5 Допущено ошибок 0:

– практическая часть: 0;

– тестовое задание: 0.

Коды аутентификации (не удалять!!! не изменять!!!):

1 Учебного модуля: CDC4BB03EC99E2E537E95FE096846511;

2 Студента: 10A5405BC829F82CC30CF22036A17717;

3 Результатов: 6C5CF6B6DB4E9DC09C5199C35057BADE.