Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет инфокоммуникаций
Кафедра защиты информации

Тема работы:

DES В РЕЖИМЕ ЗАШИФРОВАНИЯ ДАННЫХ

Вариант №17

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

Минск 2022

Цель: изучение схемы зашифрования данных DES.

Краткие теоретические сведения.

Структурная схема алгоритма DES в режиме зашифрования данных приведена на рисунке 1.

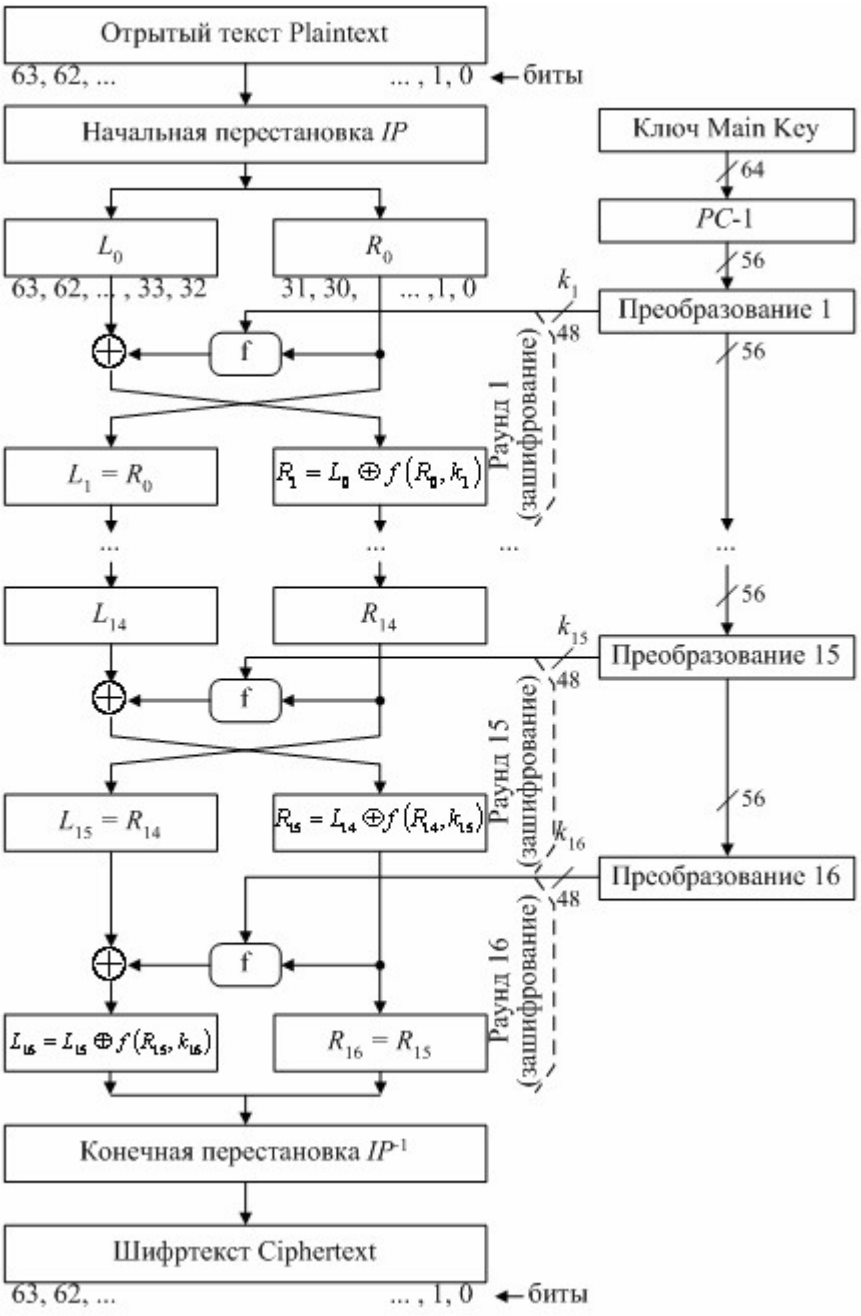


Рисунок 1 - Структурная схема алгоритма DES в режиме зашифрования данных

Алгоритм DES использует комбинацию подстановок и перестановок и осуществляет шифрование 64-битовых блоков данных с помощью 64-битового ключа, в котором значащими являются 56 бит.

Процесс зашифрования данных DES заключается в следующем.

Данные, подлежащие зашифрованию (биты отрытого текста Plaintext), переставляются в соответствии с матрицей начальной перестановки *IP*. Полученная последовательность разделяется на две части: L_0 - левые или старшие биты и R_0 - правые или младшие биты, каждая из которых содержит по 32 бита.

Затем выполняется итеративный процесс зашифрования, состоящий из шестнадцати циклов (раундов). Пусть T_i - результат i-й итерации (i = 1, 2, …, 16). Тогда

$$T_i = L_i R_i, \tag{1}$$

где $L_i = t_1, t_2, \ldots, t_{32}$ - первые 32 бита;

$R_i = t_{33}, t_{34}, \ldots, t_{64}$ - последние 32 бита.

Результат i-й итерации L_iR_i описывается следующими системами:

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, k_i) \end{cases}, i = 1,2,\ldots,15;$$

$$\begin{cases} L_{16} = L_{15} \oplus f(R_{15}, k_{15}) \\ R_{16} = R_{15} \end{cases} \tag{2}$$

Функция f называется функцией шифрования. Ее аргументами являются последовательность R_{i-1}, получаемая на предыдущем шаге итерации, и

48-битовый раундовый ключ k_i, который является результатом преобразования 64-битового секретного ключа Main Key.

На последнем шаге итерации получают последовательности R_{16} и L_{16} (без перестановки местами), которые конкатенируются в 64-битовую последовательность $R_{16}L_{16}$.

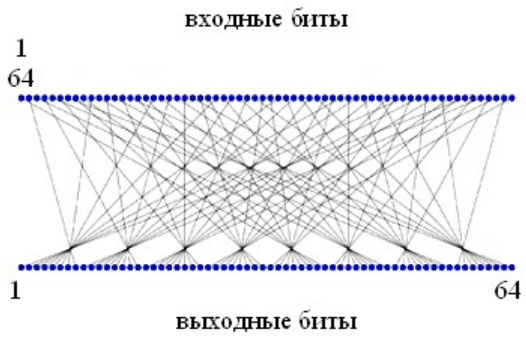
По окончании шифрования осуществляется восстановление позиций битов с помощью матрицы конечной перестановки IP^{-1}, в результате чего формируется шифртекст Ciphertext (см. рисунок 1).

Матрицы начальной IP и конечной IP^{-1} перестановки битов.

Матрицы начальной и конечной перестановки битов поясняются рисунком 2.

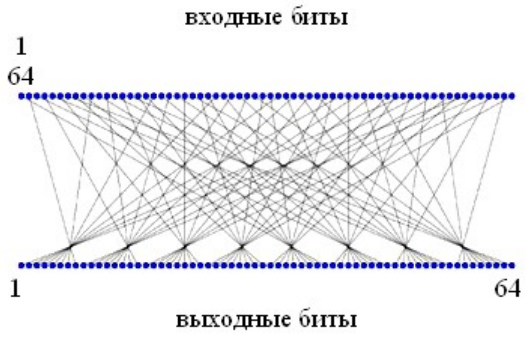
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

а)



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

б)



а) - начальная перестановка *IP*; б) - конечная (обратная) перестановка IP^{-1}

Рисунок 2 - Матрицы начальной и конечной перестановки битов

Биты входного блока Plaintext (64 бита) переставляются в соответствии с матрицей *IP*: бит 58 Plaintext становится битом 1, бит 50 - битом 2 и т.д. По

окончании шестнадцати раундов шифрования осуществляется восстановление позиций битов с помощью матрицы обратной перестановки IP^{-1}, показанной на рисунке 2, б: бит 40 становится битом 1, бит 8 - битом 2 и т.д.

Функция шифрования f.

Схема вычисления функции шифрования $f(R_{i-1}, k_i)$ показана на рисунке 3.

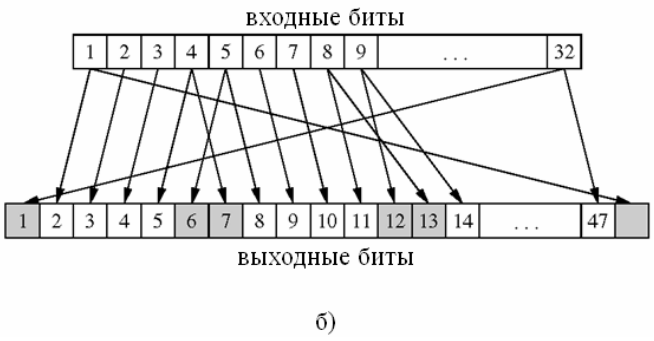
Рисунок 3 - Схема вычисления функции шифрования f

Аргументами функции шифрования f являются R_{i-1} (32 бита) и k_i (48 бит). Функция f, в свою очередь, содержит три функции: расширения E, преобразования S и перестановки P.

Функция расширения E увеличивает количество бит правой части R_{i-1} с 32-х до 48 в соответствии с правилами, иллюстрируемыми рисунком 4.

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

а)



б)

а) - матрица функции E; б) - пример преобразования входных битов в выходные

Рисунок 4 - Вычисление функции расширения E

Полученный результат $E(R_{i-1})$ складывается по модулю 2 с текущим значением раундового ключа k_i и затем разбивается на восемь 6-битовых блоков B_1, B_2,…, B_8. Далее каждый из этих блоков используется как номер элемента в функции преобразования S, содержащей восемь матриц S_1, S_2,…, S_8. Вычисление функции преобразования S поясняется рисунком 4.

номер строки	номер столбца																
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
	2	4	1	14	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	S_2
	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	S_3
	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	S_4
	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	S_5
	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	S_6
	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	11	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	S_7
	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	S_8
	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	

значения приведены в десятичном коде

Рисунок 5 - Функция преобразования S

Пусть на вход матрицы S_j поступает 6-битовый блок $B_j = b_1\ b_2\ b_3\ b_4\ b_5\ b_6$, тогда 2-битовое число $b_1\ b_6$ указывает номер строки матрицы, а 4-битовое число $b_2\ b_3\ b_4\ b_5$ - номер столбца. В результате получаем $S_1(B_1)\ S_2(B_2)\ \ldots\ S_8(B_8)$ в виде 32-битового блока, поскольку матрицы $S_1 \div S_8$ содержат 4-битовые элементы. Этот 32-битовый блок преобразуется с помощью функции перестановки P, приведенной на рисунке 6.

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

Рисунок 6 - Функция перестановки P

Как видно из рисунка 6, бит 16 становится первым выходным битом функции перестановки P, бит 7 - вторым и т.д. Выходное значение функции перестановки P является результатом функции шифрования $f(R_{i-1}, k_i)$.

Полученные результаты практических расчетов:

– L_0R_0 = FA1FCE2B89C843C3;

– L_1R_1 = 89C843C3DCB6254C;

– L_2R_2 = DCB6254C55A73212;

– L_3R_3 = 55A73212653944CE;

результаты, полученные средствами автогенерации учебного модуля:

– L_4R_4 = 653944CE148E0657;

– L_5R_5 = 148E0657AA286451;

– L_6R_6 = AA286451EB404289;

– L_7R_7 = EB4042890E649162;

– L_8R_8 = 0E649162BF7A69FD;

– L_9R_9 = BF7A69FD3A966BC8;

– $L_{10}R_{10}$ = 3A966BC87F6E71D8;

– $L_{11}R_{11}$ = 7F6E71D8E2D77AC3;

– $L_{12}R_{12}$ = E2D77AC3264B1926;

– $L_{13}R_{13}$ = 264B19260C071732;

– $L_{14}R_{14}$ = 0C07173295D7BB23;

– $L_{15}R_{15}$ = 95D7BB235D4D87CA;

– $L_{16}R_{16}$ = FA0E16825D4D87CA;

– шифртекст Ciphertext = A85FBCF2C440E24B.

Контрольные вопросы:

1 В чем отличия работы схемы шифрования данных DES для различных циклов (раундов)?

Для каждого раунда используются разные ключи, последний раунд отличается от предыдущих, R15=R16

2 Какие режимы работы определены для стандарта DES?

ECB – Электронная кодовая книга;

CBC – Сцепление блоков шифра ;

CFB – Обратная связь по шифртексту;

OFB –Обратная связь по выходу.

3 Сколько блоков открытого текста необходимо использовать при реализации схемы шифрования данных DES, если общий размер открытого текста Plaintext составляет 1 Мбайт? Какую общую длину будет иметь шифртекст Ciphertext, полученный на выходе схемы шифрования данных DES?

Если Plaintext – 1 Мбайт, значит Ciphertext тоже 1 Мбайт.

1 Мбайт/64 бит = 125тыс. блоков открытого текста.

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

5 Какова вычислительная сложность реализации схемы шифрования данных 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.

Выводы по результатам выполнения работы:

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

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

1 Дата и время: 08.12.2022 17:43;

2 Вариант №: 17;

3 Студент: Савченко Савич;

4 Номер группы: 961401;

5 Допущено ошибок 0:

– практическая часть: 0;

– тестовое задание: 0.

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

1 Учебного модуля: 002E8391831EBAF40DA55D2166E9CB73;

2 Студента: 5116DD18C196A32D2C36E5513A98D84A;

3 Результатов: 428FC33E1A649FCA22CC153742D84447.