Лабораторная работа № 2.

Стандарт DES

Американский стандарт криптографического закрытия данных DES (Data Encryption Standard), принятый в 1978 году, является типичным представителем семейства блочных шифров. Основанный на методе Фейстела, DES осуществляет шифрование 64-битовых блоков данных с помощью 56-битового ключа. Дешифрование в DES является операцией обратной шифрованию и выполняется путем повторения операций шифрования в обратной последовательности. Процесс шифрования заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах шифрования и, наконец, обратной перестановке битов (рис.3).

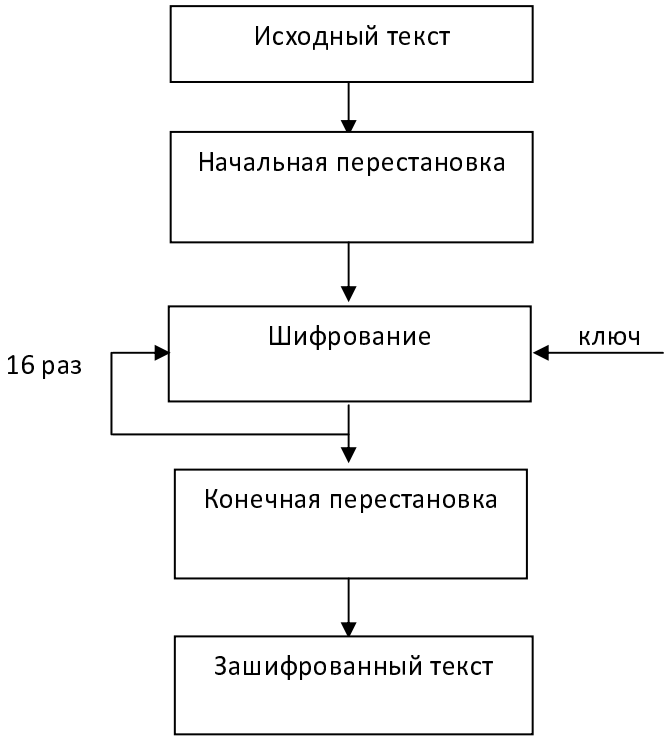

Рис. 3. Шифратор DES

Матрица P начальной перестановки имеет вид

```
58  50  42  34  26  18  10  02
60  52  44  36  28  20  12  04
62  54  46  38  30  22  14  06
64  56  48  40  32  24  16  08
57  49  41  33  25  17  09  01
59  51  43  35  27  19  11  03
61  53  45  37  29  21  13  05
63  55  47  39  31  23  15  07
```

Из файла считывается очередной 8-байтовый блок T, который преобразуется с помощью матрицы P начальной перестановки, т.е. бит с номером 58 блока T становится битом с номером 1, бит с номером 50 - битом с номером 2 и т.д., что даст в результате: $T(0) = P(T)$. Затем полученная последовательность битов T(0) делится на две последовательности по 32 бита каждая: $L(0)$ - левые или старшие биты, $R(0)$ - правые или младшие биты. Затем выполняется шифрование по методу Фейстела с 16 итерациями, как показано на Рис.4, i-я итерация описывается следующим образом

$$L(i) = R(i-1)$$

$$R(i) = L(i-1) \oplus F\left(R(i-1), K(i)\right),$$

где $L(i)$ и $R(i)$ - это левая и правая подпоследовательности на iм такте, $K(i)$ - 48 битный ключ, полученный из 64 битного ключа. На 16-й итерации получают последовательности $R(16)$ и $L(16)$ (без перестановки), которые соединяют в 64-битовую последовательность $(R(16), L(16))$. Затем биты этой последовательности переставляют в соответствии с матрицей обратной перестановки P^{-1}

40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25

Матрицы P^{-1} и P соотносятся следующим образом: значение 1-го элемента матрицы P^{-1} равно 40, а значение 40-го элемента матрицы P равно 1, значение 2-го элемента матрицы P^{-1} равно 8, а значение 8-го элемента матрицы P равно 2 и т.д.

На i-й итерации K(i) - это 48 битовый ключ, получаемый из 64 битового исходного ключа следующим образом: перед началом итераций из 64 битового ключа получают 56 битовый путем выбрасывания каждого восьмого бита, т.е. битов стоящих на позициях 8, 16, 24, 32, 40, 48, 56, 64. Эти биты были сформированы как биты контроля четности и используются для контроля целостности ключа. Затем производится начальная перестановка 56 битового ключа в соответствии с таблицей G

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

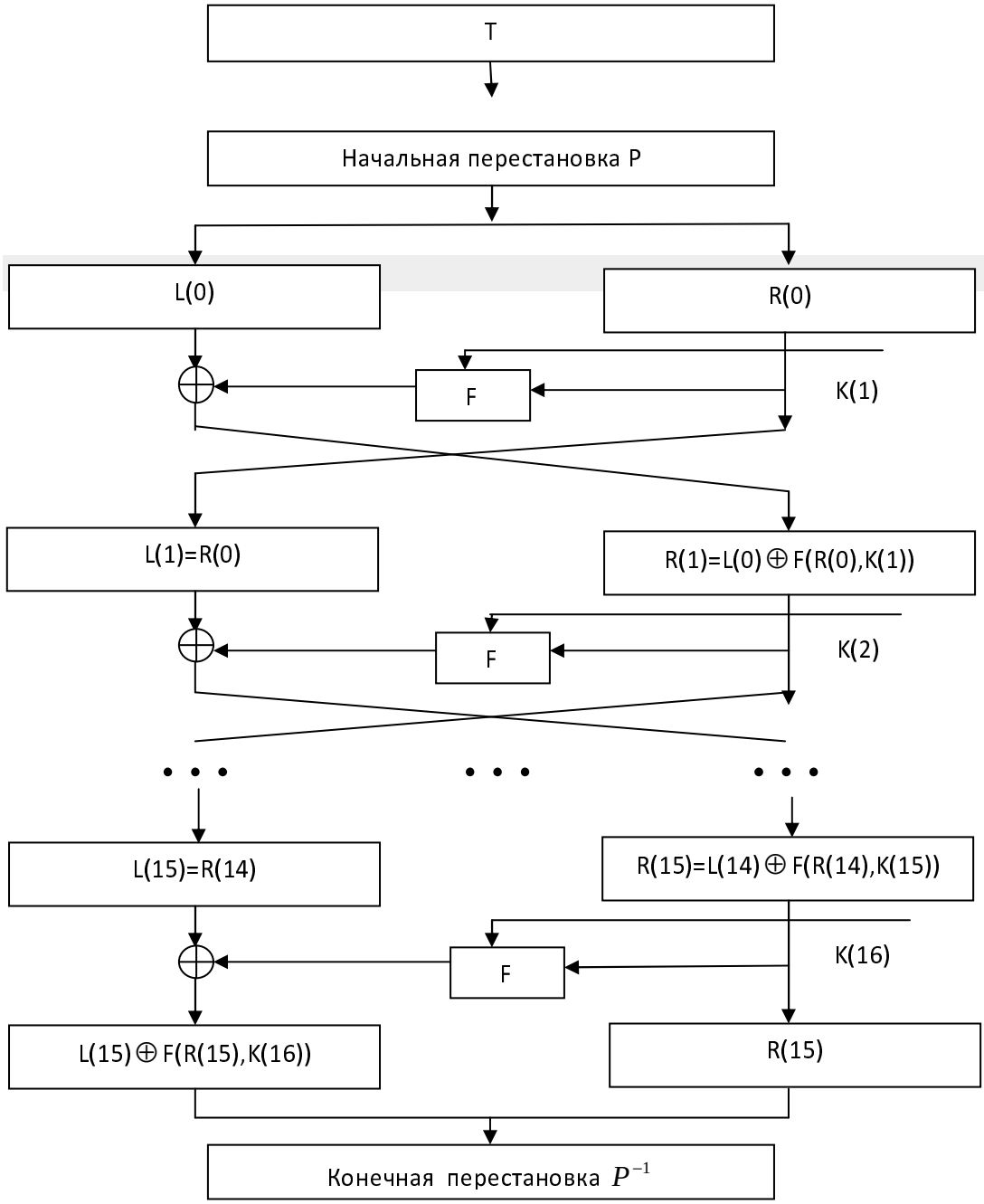

Рис. 4. Схема шифратора DES

Получаемый таким образом, 56 битовый ключ разбивается на два 28 битовых блока: C(0) – левый, и D(0) - правый. Производится левый циклический сдвиг C(0) и D(0) на заданное таблицей 1 число позиций. Из конкатенации полученных при этом блоков C(1) и D(1) выбираются 48 разрядов с помощью перестановки KP:

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

Эти разряды используются на первой итерации. На *i*-й итерации для получения блоков C(i), D(i) производится циклический сдвиг блоков C(i-1), D(i-1) на s(i) позиций, где s(i) выбирается по таблице

Таблица 1. Циклические сдвиги для 16 итераций

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
s	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Далее вновь выбираем 48 разрядов ключа с помощью перестановки KP.

Блок-схема алгоритма вычисления ключа приведена на рис. 5.

Теперь рассмотрим функцию шифрования F (R(i-1),K(i)) в стандарте DES. Она схематически показана на Рис. 6

Для вычисления значения функции F используются следующие функции-матрицы:

- E - расширение 32-битовой последовательности до 48-битовой,
- S1, S2, ... , S8 - преобразование 6-битового блока в 4-битовый,
- P2 - перестановка бит в 32-битовой последовательности.

Функция расширения E определяется следующей таблицей

```
32  01  02  03  04  05
04  05  06  07  08  09
08  09  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  01
```

Результат расширения E(R(i-1)) представляет собой 48-битовую последовательность, которая складывается по модулю 2 с 48-битовым ключом K(i). Результирующая 48-битовая последовательность делится на 8 блоков B(1),B(2),…,B(8) по 6 битов каждый, т.е. E(R(i-1)) xor K(i) = B(1)B(2)...B(8). Предположим, что на вход функции-матрицы Sj поступает 6-битовый блок B(j)=(b1,b2,b3,b4,b5,b6). Тогда биты (b1,b6) определяют номер строки в матрице, оисывающей Sj, а биты (b2,b3,b4,b5) определяют номер столбца в этой матрице (см. таблицу 2). Выходом блока Sj будет 4-битовый элемент, стоящий на пересечении соответствующей строки и столбца.

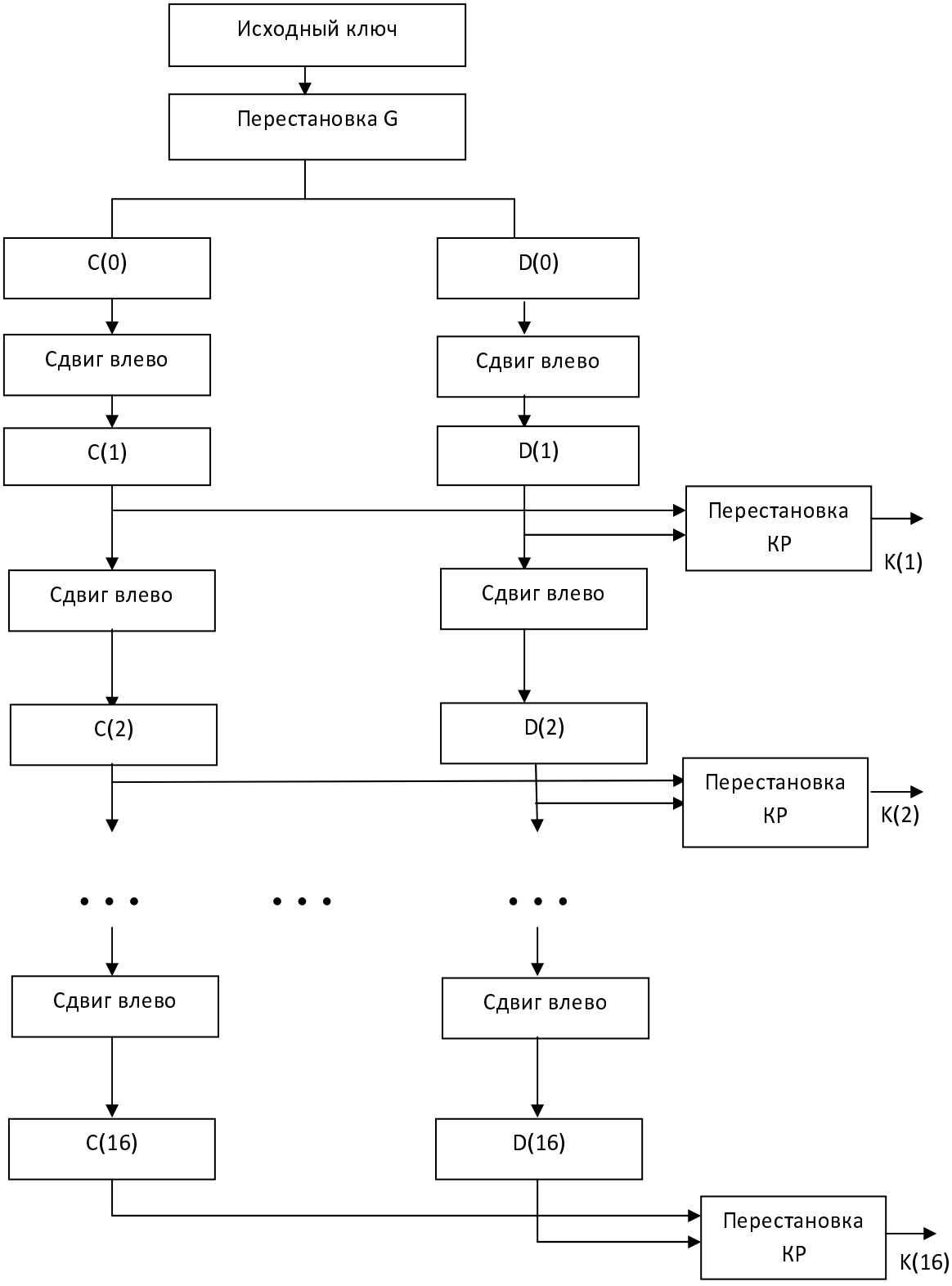

Рис 5. Схема формирования ключей

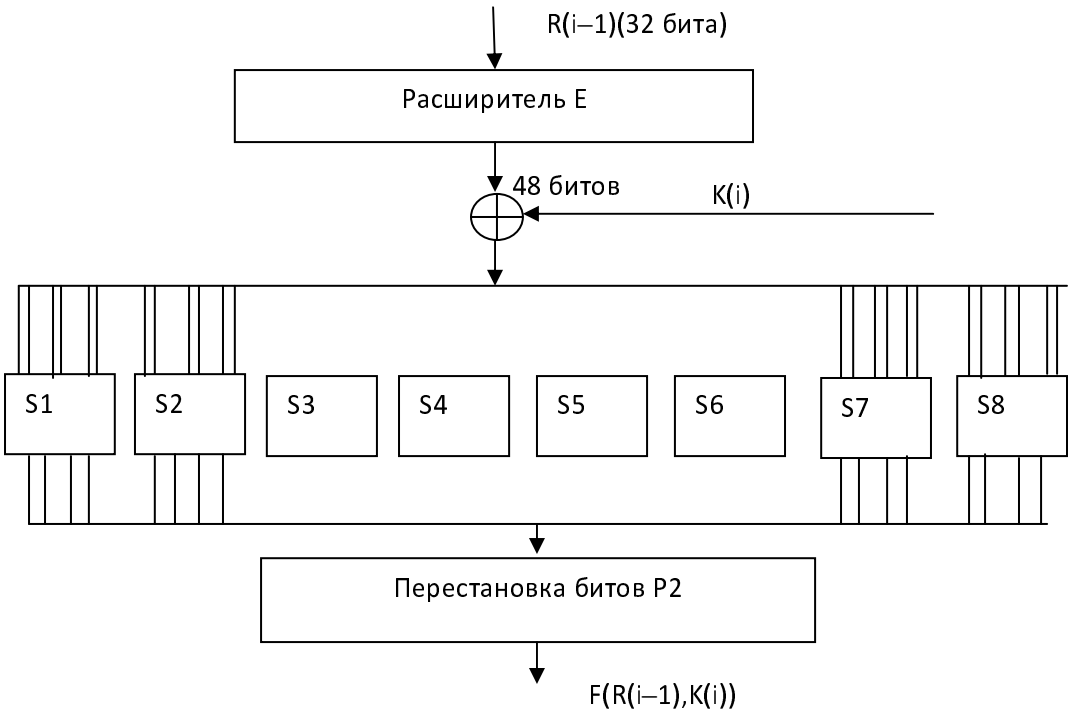

Рис. 6. Функция шифрования

Например, пусть B(1)=(010111), тогда номер строки равен 1, а номер столбца 11, т.е. в матрице S1 находим элемент, стоящий на пересечении 1-й строки и 11-го столбца. Это 11, таким образом, выход блока имеет вид 1011.

Применив преобразование к каждому из восьми 6 битовых блоков, получаем 32-битную выходную последовательность и применяем к ней перестановку P2

```
16  07  20  21
29  12  28  17
01  15  23  26
05  18  31  10
02  08  24  14
32  27  03  09
19  13  30  06
22  11  04  25
```

В результате получаем F(R(i-1), K(i)) = P2(S1(B(1)),...S8(B(8))).

Таблица 2. Функции преобразования S1, S2, ..., S8

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	
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	S1
	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	
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	S2
	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	S3
	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	S4
	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	S5
	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	S6
	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	
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	S7
	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	S8
	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	

DES неоднократно подвергался критике из-за малой длины ключа, а в 1998 году атака по данной паре «открытый текст – шифртекст» оказалась успешной. Среднее время вскрытия ключа составило около 3 суток. В связи с этим было выдвинуто несколько предложений по усовершенствованию системы DES.

Первое предложение состояло в использовании DES дважды с различными ключами, каждый из которых имеет длину 56 бит. Формально общая длина ключа в такой системе равна 112 битам, однако, легко показать, что сложность вскрытия ключа в такой системе возрастает лишь в 2 раза по сравнению с DES. Действительно, пусть мы выполняем двойное шифрование с ключами K_x и K_y соответственно:

$$Y = DES_{K_y}(DES_{K_x}(X)).$$

В этом случае система оказывается неустойчива по отношению к атаке “meet-in-the-middle” (встреча посередине). Опишем эту атаку. Пусть в нашем распоряжении имеется открытый текст X_1 и шифртекст Y_1, полученный в результате двойного шифрования с помощью алгоритма DES. Зашифруем X_1 на множестве возможных ключей K_x и запишем результаты в таблицу. Расшифруем Y_1 на множестве возможных ключей K_y и также запишем результаты в таблицу. Затем будем искать совпадения в таблицах, эти совпадения соответствуют ключам - возможным кандидатам на то, чтобы быть искомыми ключами K_x и K_y. Далее перебор происходит среди этих кандидатов. Для сокращения перебора можно использовать еще одну пару – открытый текст – шифртекст и повторить атаку. В этом случае при шифровании и дешифровании мы используем только ключи-кандидаты.

Наиболее известным предложением по усилению DES является так называемый тройной DES, определяемый формулой

$$Y = DES_{K_z}(DES^{-1}_{K_y}(DES_{K_x}(X))).$$

Нетрудно видеть, что в такой системе ключ имеет длину $56 \times 3 = 168$ бит. Шифрование 64 битного блока осуществляется шифрованием с одним подключом, расшифрованием с другим и затем шифрованием с третьим. Причина того, что вторым шагом является расшифрование $DES^{-1}_{K_y}$ - совместимость с DES. Если все три ключа одинаковы, то тройной DES эквивалентен DES. Однако, тройной DES существенно медленнее DES.

Еще одна модификация DES, предложенная Р. Ривестом получила название «расширенный DES». В этом случае шифртекст получают следующим образом:

$$Y = K_y \oplus DES_K(X \oplus K_x),$$

то есть ключ включает три подключа и состоит из 54+64+64=184 бит. Ключи K_x и K_y называют предварительный и завершающий зашумляющий ключ, соответственно. В отношении этого варианта использования *DES* доказано, что он увеличивает стойкость к атаке, основанной на переборе ключей. Кроме того, он усиливает стойкость к, так называемому ***дифференциальному и линейному криптоанализу.***

Дифференциальный криптоанализ состоит в поиске корреляции между суммой по модулю 2 исходных текстов и суммой по модулю два соответствующих шифртекстов. Например, такой анализ может быть применен к результатам одного раунда сети Фейстела для определения подключа раунда. Если для многих пар входных блоков, которые имеют одно и тоже отличие Λ_X разница между соответствующими шифртекстами тоже одинакова и равна Λ_Y, то можно сказать что с определенной вероятностью Λ_Y следует из Λ_X и, следовательно, подключ раунда известен с этой вероятностью. Так как раунды независимы, то вероятности определения ключей раундов следует перемножать, чтобы определить вероятность взлома системы шифрования в целом.

Линейный криптоанализ предполагает построение и решение линейных уравнений следующего вида. Если выполнить операцию сложения по модулю два некоторых битов открытого текста и некоторых битов шифртекста, то получаем сумму по модулю два некоторых битов ключа. Уравнение выполняется с некоторой вероятностью, которую оценивают, используя большое количество открытых текстов и соответствующих шифртекстов.

ЗАДАНИЕ

1. Зашифровать текст по алгоритму шифрования стандарта DES.
2. Расшифровать текст зашифрованный по стандарту DES с заданным ключом.

ИСХОДНЫЕ ДАННЫЕ: Файл с открытым текстом.

СОДЕРЖАНИЕ ОТЧЕТА: Отчет по лабораторной работе должен содержать

1. Описание алгоритма шифрования
2. Описание алгоритма дешифрования
3. Исходный и зашифрованный текст