Блочные шифры — это шифры, которые осуществляют изменение информации блоками фиксированной длины.

При использовании блочного шифра данные представляются как последовательность n-битовых блоков. Если в последнем блоке не хватает необходимого количества битов, то этот блок обычно дополняется конструкцией вида «100...0› до необходимого количества.

При блочном шифровании открытый текст можно представить в виде $M_1 M_2 M_3 \ldots M_n$, где M_i — отдельные блоки, преобразуемые независимо от остальных. Обычно длина входного блока совпадает с длиной выходного блока, т. в. можно сказать, что блочный шифр задает взаимно однозначное соответствие между входным и выходным блоками.

Блочный шифр преобразует блок открытою текста фиксированной длины в блок криптограммы такой же длины используя какую—либо функцию шифрования по какому-либо ключу.

Пусть $E_k (T)$ — функция шифрования, тогда, если сообщение состоит из m n-битовых блоков, то можно записать таблицу подстановки:

1	**2**	**3**	**…**	**n**
$E_1 (T)$	$E_2 (T)$	$E_3 (T)$	…	$E_n (T)$

Различным ключам соответствуют различные таблицы подстановки.

Пример

Пусть функция шифрования определяется как $f(k) = 2k^n$, где k — соответствующий ключ, а n —— номер очередного блока.

Пусть имеется набор ключей: {2, 3, 4, 5} и четыре блока для шифрования. Требуется получить таблицу подстановки для каждого ключа.

Решение

Решая уравнение $f(k) = 2k^n$ относительно каждого конкретного ключа и номера блока, получаем следующие таблицы подстановки:

n	1	2	3	4
k	4,6,8,10	8,18,32,50	16,54,128,250	32,162,512,1250

Американский стандарт шифрования данных DES

В качестве американском стандарта шифрования данных в середине 1970-х гг. Национальным институтом стандартов и технологий была принята система шифрования

DES. Данная система широко применялась (и иногда применяется в наши дни) во всем мире, особенно в финансовой сфере.

Система шифрования DES была создана в 1972—1975 гг. в исследовательской лаборатории корпорации IBM группой под руководством доктора У. Тачмена. В качестве федерального стандарта США данная криптосистема была принята в 1977 г. (эта система не была запатентована).

Система DES – блочный шифр, где размер блока составляет 64 бита. В системе используются 56 – битовые ключи.

Общая схема алгоритма DES

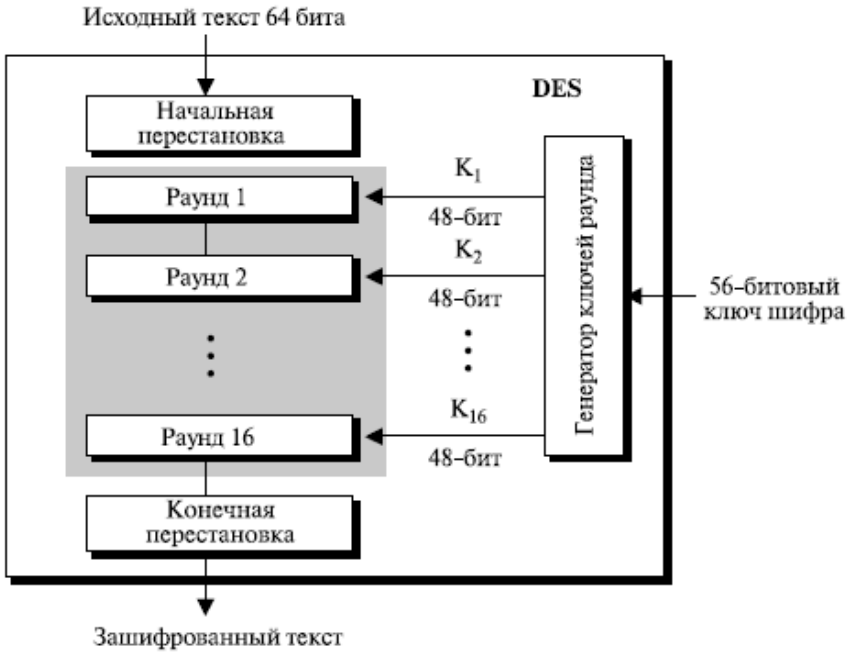
1. б4-битовый блок открытого текста после начальной перестановки делится на две равные части по 32 бита. Назовем эти под-блоки L и R.
2. Над каждой парой блоков выполняется 16 раундов шифровании вида:

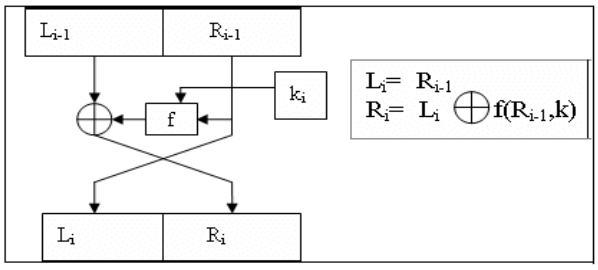
$$L_i = R_{i-1};$$

$$R_i = L_{i-1} \otimes F(R_{i-1}, K_i),$$

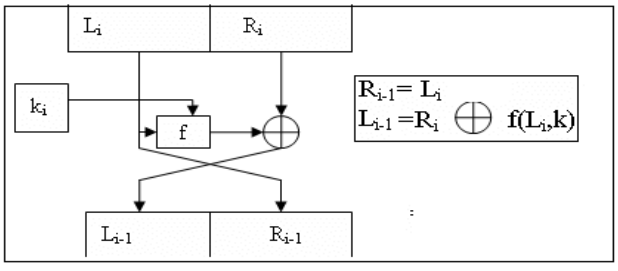
где знак $\otimes$ означает операцию поразрядного суммирования.

Рассмотрим этот алгоритм шифрования подробнее.





Прямое преобразование (шифрование)



Обратное преобразование (расшифрование)

1. Выполняем перестановку вида:

Начальные перестановки							
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

2. Разбиваем блок пополам.
3. Расширяем под-блок R в 48-битовый под-блок. Для этого разбиваем его на 4-битовые под-блоки, затем в начало и конец каждого под-блока дописываем по одному биту согласно таблице расширения:

Таблица расширения					
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**

Каждая строка таблицы представляет собой расширенный (6-битовый) под-блок. Жирным шрифтом выделены те биты исходного 48-битового под-блока, за счет которых производится расширение.

4. Выполняем линейное преобразование — поразрядное суммирование по модулю 2

$$F(R_{i-1}, K_i)$$

5. Выполняем 8 операций подстановки. Для каждой операции используется одна из 8 таблиц подстановки размером 4x16. К каждому отдельному блоку применяется одна конкретная подстановка. На основе 6-битового входного под-блока формируются два двоичных вектора v1 и v2. Вектор v1 представляет собой 2-битовый под-блок, содержащий 1-й и 6-й биты входного под-блока. Вектор v2 содержит 4 средних бита входного под-блока. Используя одну из таблиц подстановки находим число, стоящее на пересечении строки с номером v1 и столбца с номером v2. Это число, записанное в двоичном виде, и является выходным под-блоком.

6. Записываем полученные под-блоки в один блок и производим поразрядное суммирование по модулю 2 полученной последовательности с левым блоком:

$$L_{i-1} \otimes F(R_{i-1}, K_i)$$

7. Выполняем операцию перестановки вида:

Конечные перестановки							
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

Пример таблицы подстановки (пункт 5):

00		14	4	13	1	2	15	11	8
01		0	15	7	4	14	2	13	1
10		4	1	14	8	13	6	2	11
11		15	12	8	2	4	9	1	7
v1	**v2**	**0000**	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**

00		3	10	6	12	5	9	0	7
01		10	6	12	11	9	5	3	8
10		15	12	9	7	3	10	5	0
11		5	11	3	14	10	0	6	13
v1	**v2**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**

Пример раунда шифрования

Пусть имеется 64-битовый блок после выполнения операции перестановки:

10011010100010111010010001001111
01101011101101011111001101101011

Разбиваем его на блоки L и R:

$$L = 10011010100010111010010001001111;$$
$$R = 01101011101101011111001101101011.$$

Разбиваем блок R на 4-битвые под-блоки:

0110 1011 1011 0101 1111 0011 0110 1011.

Расширяем под-блоки до 6 битов, используя приведенную выше таблицу расширения:

101101 010111 110110 101011 111110 100110 101101 010110.

Выбираем ключ (случайный):

100101011001010101001100100111100101100100111111.

Производим операцию поразрядного суммирования:

$$
\begin{array}{ll}
 & 101101\ 010111\ 110110\ 101011\ 111110\ 100110\ 101101\ 010110 \\
+ & 100101\ 011001\ 010101\ 001100\ 100111\ 100101\ 100100\ 111111 \\
\hline
 & 001000\ 001110\ 100011\ 100111\ 011001\ 000011\ 001001\ 101001
\end{array}
$$

Используя приведенную выше таблицу подстановки. получаем выходной блок $F(R_{i-1}, K_i)$:

00101000110000101001111111100100.

Производим операцию поразрядного суммирования с исходным блоком L. Получаем выходной R-блок:

$$
\begin{array}{ll}
 & 00101000\ 11000010\ 10011111\ 11100100 \\
+ & 10011010\ 10001011\ 10100100\ 01001111 \\
\hline
 & 10110010\ 01001001\ 00111011\ 10101011
\end{array}
$$

Соединяем блоки R и L н выполняем операцию перестановки.

Слабости алгоритма DES

В структуре блоков начальной и первичной перестановки были найдены одна загадка и одна слабость.

Не ясно, почему проектировщики DES использовали начальную и конечную перестановки. Эти перестановки не вносят никаких новых свойств с точки зрения безопасности.

В перестановке расширения (в функции) первые и четвертые биты последовательностей на 4 бита повторяются.

Так же, к одной из слабостей DES является размер ключа 56 битов. Чтобы предпринять атаку грубой силы данного блока зашифрованного текста, злоумышленники должны проверить 256 ключей. Используя доступную сегодня технологию, можно проверить один миллион ключей в секунду. В 1998 году был создан специальный компьютер, с помощью которого ключ был найден за 112 часов.

Компьютерные сети могут моделировать параллельную обработку. В 1977 году команда исследователей использовала 3500 компьютеров, подключенных к Internet, чтобы найти ключ RSA за 120 дней. Множество ключей было разделено среди всех этих компьютеров, и каждый компьютер был ответственен за проверку части домена DES. Если 3500 связанных в сеть компьютеров могут найти ключ через 120 дней, сеть из 42 000 компьютеров может найти ключ через 10 дней.

DES, как первый блочный шифр, имеющий важное значение, прошел через много испытаний на безопасность. Среди предпринятых атак лишь три представляют интерес: грубая сила, дифференциальный криптоанализ и линейный криптоанализ.

Атака грубой силы

Мы уже обсуждали слабость шифра с коротким ключом. Слабость ключа совместно с другими рассмотренными недостатками, делает очевидным, что DES может быть взломан с числом испытаний 255. Однако сегодня большинство приложений использует либо 3DES с двумя ключами (размер ключа 2^{112}), либо 3DES с тремя ключами (размер ключа 2^{168}). Эти две многократных версии DES позволяют ему показывать существенную стойкость к атакам грубой силы.

Дифференциальный криптоанализ

DES не является устойчивым к такому виду атаки. Сегодня доказано, что DES может быть взломан, используя дифференциальный криптоанализ, если мы имеем 2^{47} выборок исходного текста или 2^{55} известных исходных текстов. Хотя это выглядит более эффективно, чем в атаке грубой силы, предположить, что кто-то знает 2^{47} выборок исходного текста или 2^{55} выборок исходного текста, практически невозможно. Поэтому мы можем сказать, что DES является стойким к дифференциальному криптоанализу. Также показано, что увеличение числа раундов до 20 увеличивает число требуемых выборок исходного текста для атаки более чем до 2^{64}. Такое увеличение невозможно, потому что число блоков исходного текста в DES только 2^{64}.

Линейный криптоанализ

Линейный криптоанализ — более новая методика, чем дифференциальный криптоанализ. DES более уязвим к применению линейного криптоанализа, чем к дифференциальному криптоанализу — вероятно потому, что этот тип атак не был известен проектировщикам DES. Показано, что DES может быть взломан с использованием 2^{43} пары известных исходных текстов. Однако с практической точки зрения перехват такого количества пар очень маловероятен.

Задание на лабораторную работу

1) Для функции шифрования f(k) = 2 + k × n и набора ключей {1, 4, 6, 12, 13, 46, 78} составить все таблицы подстановок.
2) Для функции f(k) = 101110110100011010 + k + 2n и записанных в двоичном виде ключей 252178, 153722, 157646 получите таблицы подстановок. (Выражение 2n переведите в двоичный код)
3) Пользуясь расширенной таблицей ASCII-кодов, получите двоичный код для фразы *«без труда не вытащишь и рыбку из пруда».* Используя вышеприведённую таблицу подстановок и сгенерированный ключ (см. приложение -> режим «1 раунд»), зашифруйте полученный набор битов с помощью ОДНОГО раунда шифрования DES. (Таблица подстановки используется одна на все блоки)
4) Придумайте фразу на русском языке длинной не более 32 символов. Проведите ОДИН раунд шифрования придуманного текста (Таблица подстановки используется одна на все блоки).
5) Предоставить программную реализацию алгоритма DES на любом удобном языке программирования.