КМиСЗИ

Лекция 1

К.т.н., доц. каф. КИБЭВС

Костюченко Евгений Юрьевич

Криптография

Криптография—это наука, занимающаяся поиском и исследованием математических методов преобразования информации с целью ее защиты

Криптография, наряду с криптоанализом (наукой о взломе шифров), является составной частью криптологии.

Криптология – наука о математических аспектах защиты информации, изучающая как сами методы защиты, так и методы противодействия им.

Применяемые в криптографии алгоритмы

1. Алгоритмы с закрытым ключом
2. Алгоритмы с открытым ключом
3. Бесключевые алгоритмы

Классификация алгоритмов

- Симметричные
  - Блочные шифры
    - Алгоритмы перестановки
    - Алгоритмы замены
    - Шифры гаммирования
    - Композиционные
  - Поточные шифры
    - Синхронные
    - Самосинхронизирующиеся
  - Комбинированные
- Асимметричные

Алгоритмы перестановки

При использовании алгоритмов перестановки в сообщения, как правило, не вводится новых знаков и состав имеющихся знаков не изменяется. Защита информации осуществляется на основе перемешивания имеющихся знаков сообщения. Анаграммы применялись, например, для сообщений об открытиях.

Пример – простейшее шифровальное устройство – скитала.

Алгоритм замены

Заключается в замене знаков сообщения на другие по определенному принципу. Простейший пример – шифр Цезаря. Заключается в сдвиге буквы на заданное количество позиций.

Квадрат Полибия

	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						

Шифр Вижинера

Шифры гаммирования

С другой стороны одноразовый блокнот может быть рассмотрен как шифр гаммирования. В рамках такого текста блок шифр-текста складывается с блоком ключа по модулю, определяемому размером блока.

Математические основы криптографии. Множества. Основные понятия

Мы будем понимать под множеством любую совокупность объектов, называемых элементами множества. Множества с конечным числом различных элементов могут быть описаны путем явного перечисления всех элементов. Обычно эти элементы заключаются в фигурные скобки. Например, {16,32,64} – множество степеней двойки, заключенных между 10 и 100. Множество обозначается прописной буквой какого-либо алфавита, а его элементы – строчными буквами того же или другого алфавита. Для некоторых особо важных множеств приняты стандартные обозначения, которых следует придерживаться. Так, буквами N, Z, Q, R обозначают соответственно множество натуральных чисел, множество целых чисел, множество рациональных чисел и множество вещественных чисел.

Множества

Целые числа

Целое число s называется делителем (или множителем) целого числа n, если $n=st$ для некоторого $t \in Z$. В свою очередь n называется кратным s. Делимость n на s обозначается символом $|$. Делимость – транзитивное свойство на Z. Целое число p, делители которого исчерпываются числами $\pm p$, ± 1 (несобственные делители), называется простым. Обычно в качестве простых берутся положительные простые числа > 1.

НОД

Наибольший общий делитель НОД(x,y) – такое максимальное число d, что ad=x и bd=y, a,b,d,x,y принадлежат N.

Функция Эйлера

Определяется следующим образом. Если натуральное число n делится в точности на k различных простых чисел p1,p2,…pk, то количество чисел, меньших n и взаимно простых с n, равно $\phi(n)=n(1-1/p1)(1-1/p2)\ldots(1-1/pk)$. Пример 4. n =1155; p1=3; p2=5; p3 =7; p4 =11. $\phi(n)=1155(1-1/3)(1-1/5)(1-1/7)(1-1/11)=480$.

Бинарные операции

Пусть X – произвольное множество. Бинарной алгебраической операцией (или законом композиции) на X называется произвольное (но фиксированное) отображение $т:X\times X\to X$ декартова квадрата $X2 = X\times X$ в X. Таким образом, любой упорядоченной паре (a,b) элементов $a,b\in X$ ставится в соответствие определенный элемент $т(a,b)$ того же множества X.

Бинарная операция * на множестве X называется ассоциативной, если $(a*b)*c=a*(b*c)$ всех $a,b,c\in X$. Она также называется коммутативной, если $a*b=b*a$. Те же названия присваиваются и соответствующей алгебраической структуре $(X,*)$. Требования ассоциативности и коммутативности независимы. В самом деле, операция * на Z, заданная правилом $n*m=-n-m$, очевидно, коммутативна. Но $(1*2)*3=(-1-2)*3=-(1-2)-1=0 \neq 1*(1*3)$. Так что условие ассоциативности не выполняется.

Элемент $e\in X$ называется единичным (или нейтральным) относительно рассматриваемой бинарной операции *, если $e*x=x*e$ для всех $x\in X$. Если e' – еще один единичный элемент, то, как следует из определения, $e'=e'*e=e$. Следовательно, в алгебраической структуре $(X,*)$ может существовать не более одного единичного элемента.

Полугруппа. Обратный элемент

Множество X с заданной на нем бинарной ассоциативной операций называется полугруппой. Полугруппу с единичным (нейтральным) элемен- том принято называть моноидом. Элемент a моноида $(M, \cdot, e)$ называется обратимым, если найдется элемент $b \in M$, для которого $a \cdot b = b \cdot a = e$ (понятно, что элемент b тоже об- ратим). Если еще и $a \cdot b' = e = b' \cdot a$, то $b' = e \cdot b' = (b \cdot a) \cdot b' = b \cdot (a \cdot b') = b \cdot e = b$. Это дает основание говорить просто об обратном элементе a^{-1} к (обратимому) элементу $a \in M: a \cdot a^{-1} = e = a^{-1} \cdot a$. Разумеется, $(a^{-1})^{-1} = a$.

Группа

Моноид G, все элементы которого обратимы, называется группой. Другими словами, предполагается выполнение следующих аксиом: (G1) на множестве G определена бинарная операция $(x,y) \to xy$; (G2) операция ассоциативна: $(xy)z=x(yz)$ для всех $x,y,z \in G$; (G3) G обладает нейтральным (единичным) элементом e: $e*x=x*e$ для всех $x \in G$; (G4) для каждого элемента $x \in G$ существует обратный x^{-1}: $x^{-1}*x = x*x^{-1}=e$.

Кольцо

Пусть K – непустое множество, на котором заданы две бинарные алгебраические операции + (сложение) и × (умножение), удовлетворяю- щие следующим условиям: К1 (K,+) – коммутативная (абелева) группа; К2 (K,×) – полугруппа; К3 операции сложения и умножения связаны дистрибутивными законами (другими словами, умножение дистрибутивно по сложению): (a+b)×c=a×c+b×c, c×(a+b)=c×a+c×b, a,b,c∈K. Тогда (K,+,×) называется кольцом. Структура (K,+) называется аддитивной группой кольца, а (K,×) – его мультипликативной полугруппой. Если (K,×) – моноид, то говорят, что (K,+,×) – кольцо с единицей.

Композиционные шифры

Используют последовательно несколько методов шифрования, как правило, из разных классов. Например, могут последовательно многократно использоваться по очереди подстановки и перемешивания. Способны обеспечивать очень высокую криптостойкость. Лежат в основе используемых стандартов шифрования DES, ГОСТ 28147-89, AES и других.

Конструкция Фейстеля

Является типовой реализацией подхода к построению блочных шрифтов.

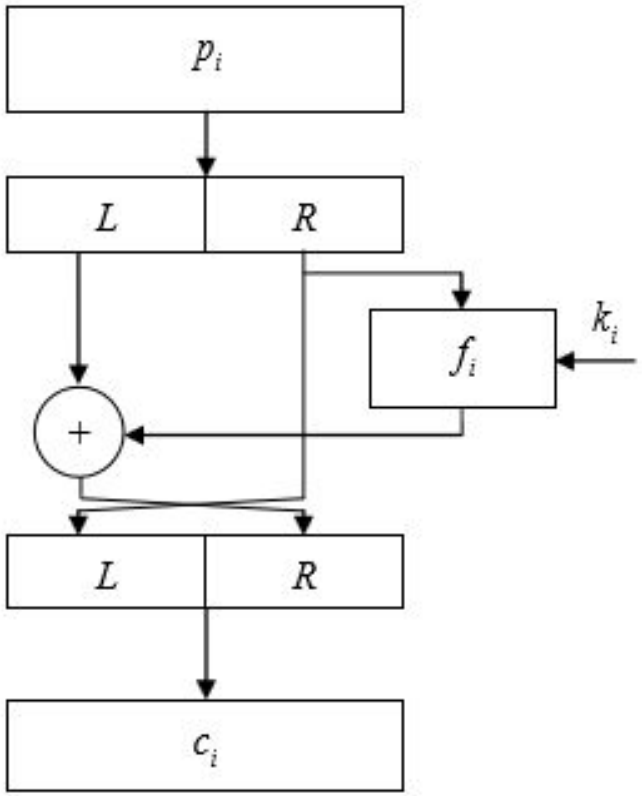
Шифрование-Расшифрование

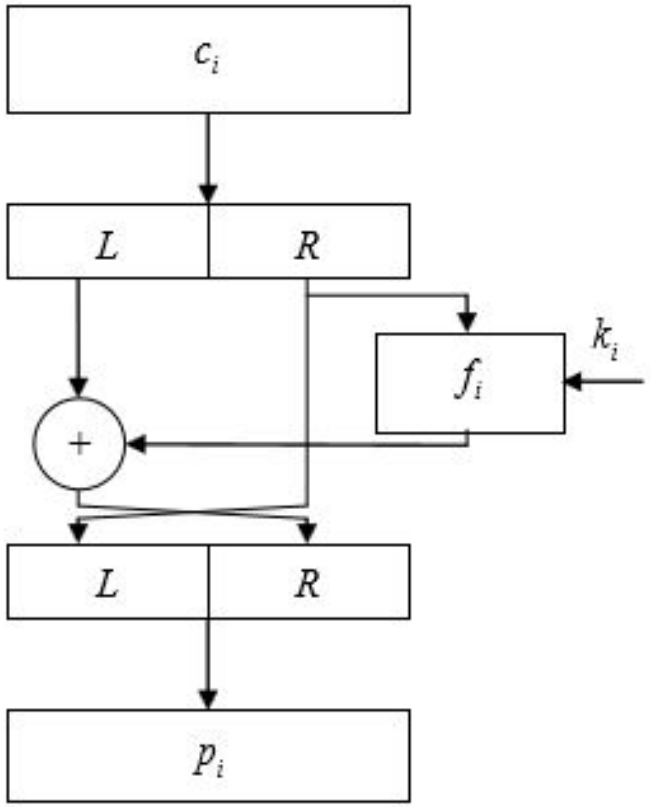
Процедуры шифрования и расшифрования аналогичны, однако ключи ki выбираются в обратном порядке.

Композиционные блочные шифры

Количество повторов в сети Фейстеля – количество раундо шифрования r. Общий ключ разбивается на r частей – раундовых ключей, участвующих отдельно в каждом раунде. Реализуется последовательно последовательность подстановок (замен) и перестановок.

Раундовая функция шифрования-дешифрования





Режим сцепления блоков шифрованного текста

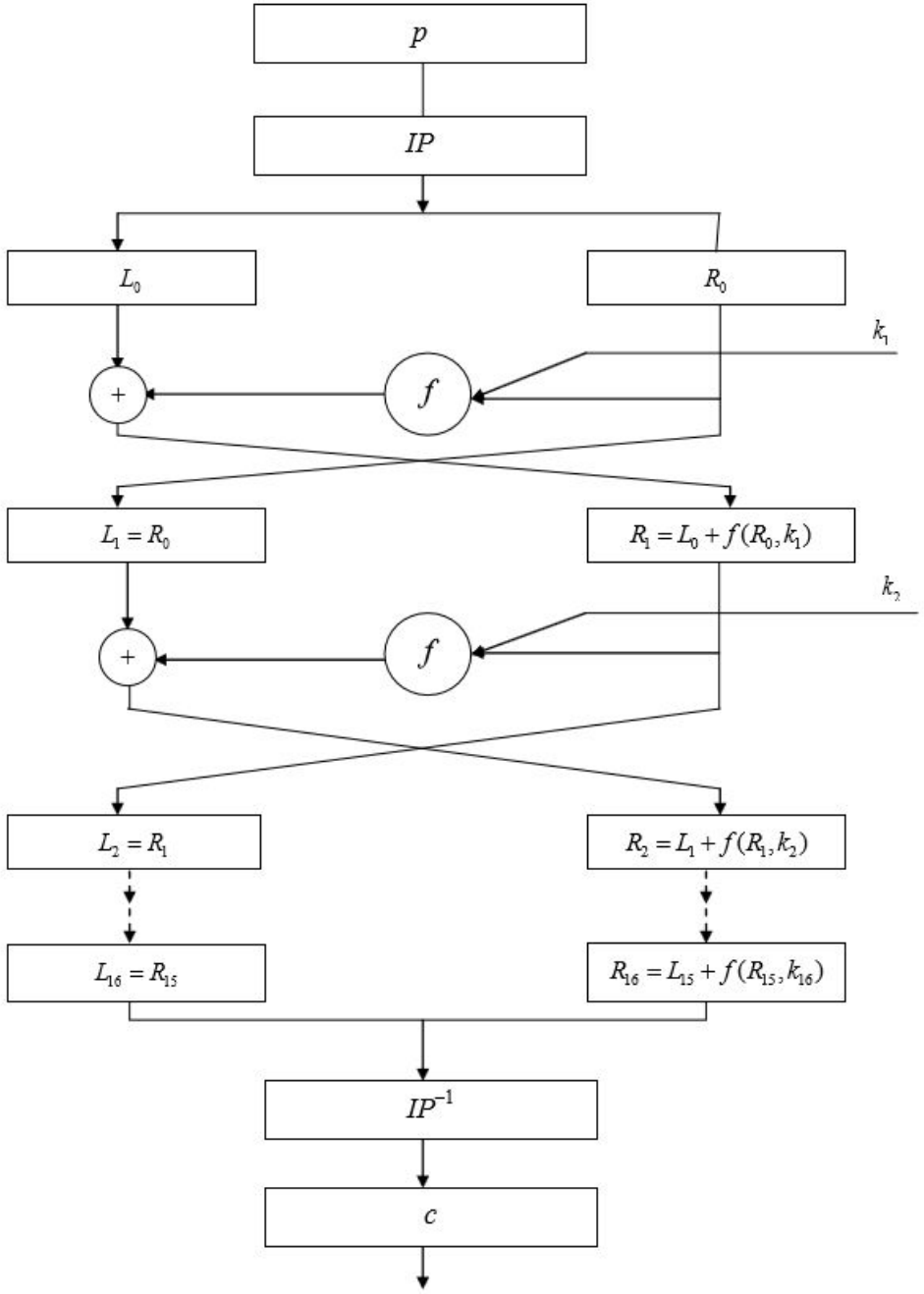
Режим обратной связи по шифрованному тексту

Шифр DES

Разновидностью шифра Фейстеля является созданный в 1974 г. шифр DES (Data Encryption Standard) и предложенный в качестве стандарта шифрования данных в государственных и частных организациях США. Шифр DES имеет длину блока исходных данных p равную 64 битам и ключ сложения по модулю 2 длиной 56 бит. Ключ, реализующий подстановку, является ключом длительного пользования, который выбирается по специальным критериям.

Шифр DES

В рамках данной схемы набор раундов по сути определяет прямую 64-битную замену 1 блока на другой. Блоки IP и
IP-1 – блоки начальной и конечной перестановок бит. f – функция криптографического преобразования, использующая при работе раундовый ключ. Количество раундов в рамках стандартного алгоритма DES равно 16. Размер блока – 64 бита. Размер ключа – 56 бит. Размер раундового ключа – 48 бит.



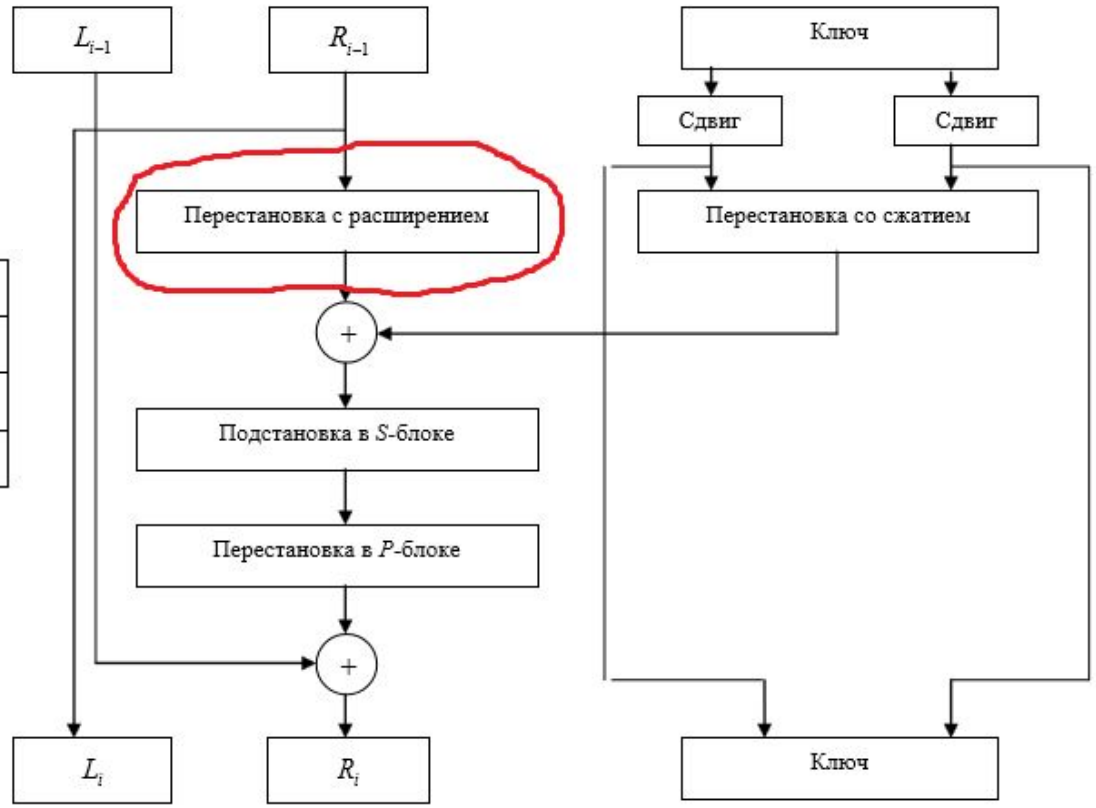
Шифр DES. Начальная перестановка.

Блок начальной таблицы перестановки бит. В соответствии с этой таблицей 58 бит открытого текста становится первым битом, 50 бит становится вторым битом, 42 бит — третьим, а первый бит открытого текста перемещается на 40 позицию и т. д.

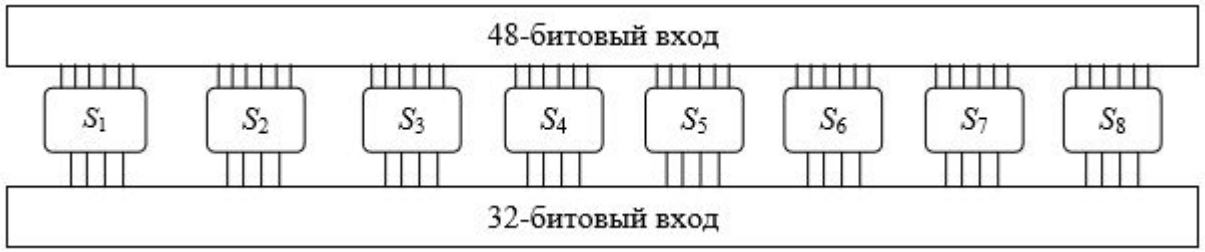
58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Шифр DES. Раундовая функция шифрования.

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



Шифр DES. Раундовая функция шифрования.

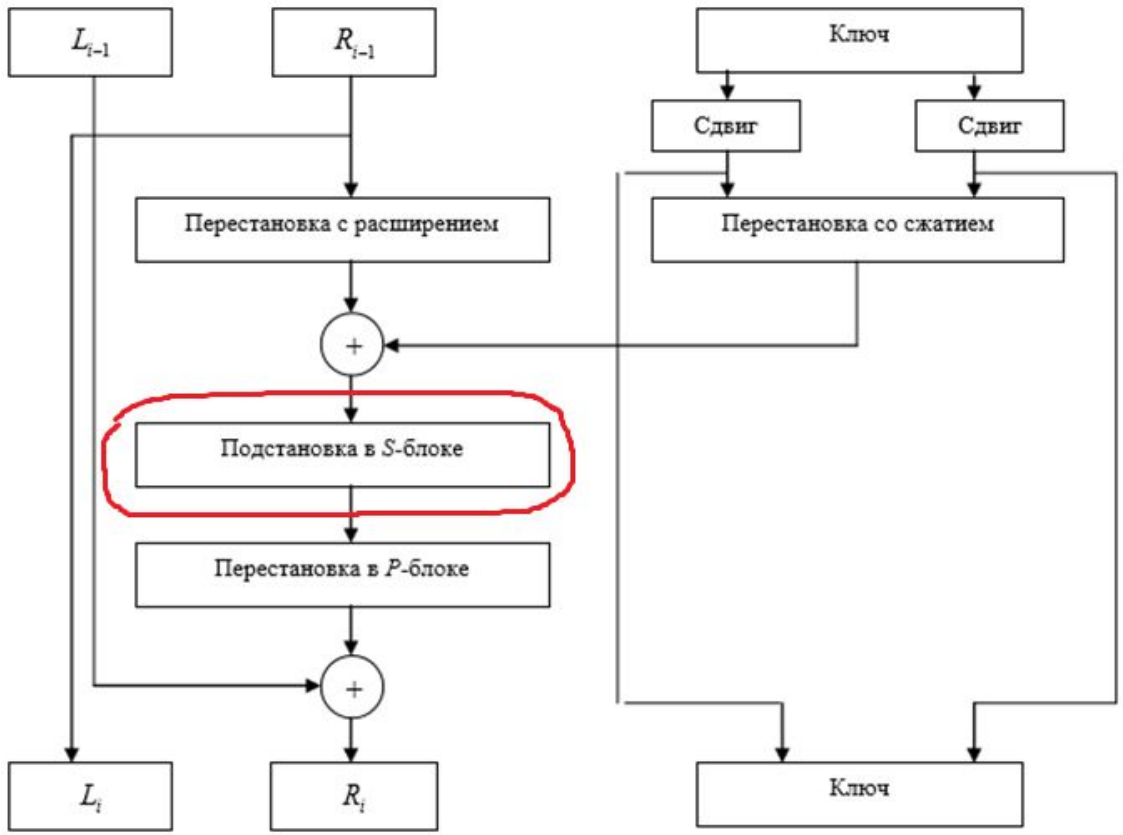


Блок замен S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Блок замен S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

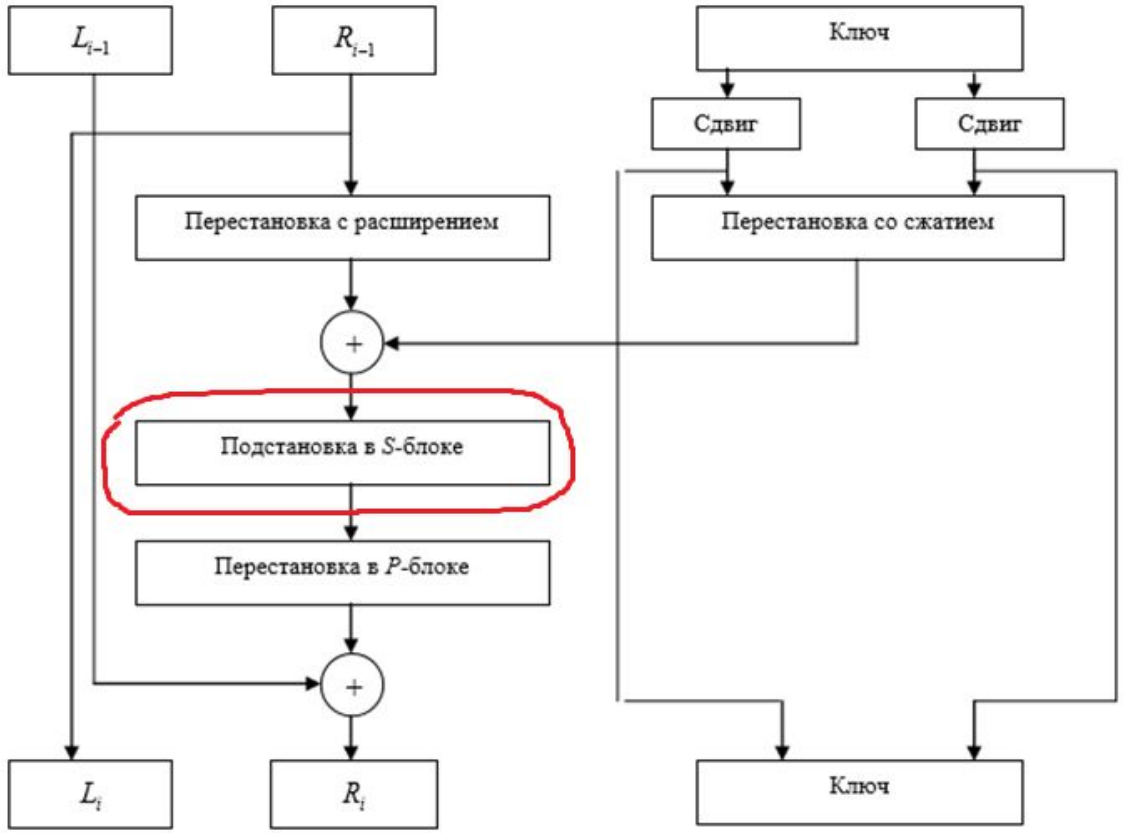


Шифр DES. Раундовая функция шифрования.

Крайний левый и крайний правый биты каждого из восьми шестиразрядных символов дают сочетание от 00 до 11, которое определяет номер используемой строки в блоке подстановки, а оставшиеся четыре символа определяют номер столбца. Итог – 8*4=32 бита (полублок)

Блок замен S_1

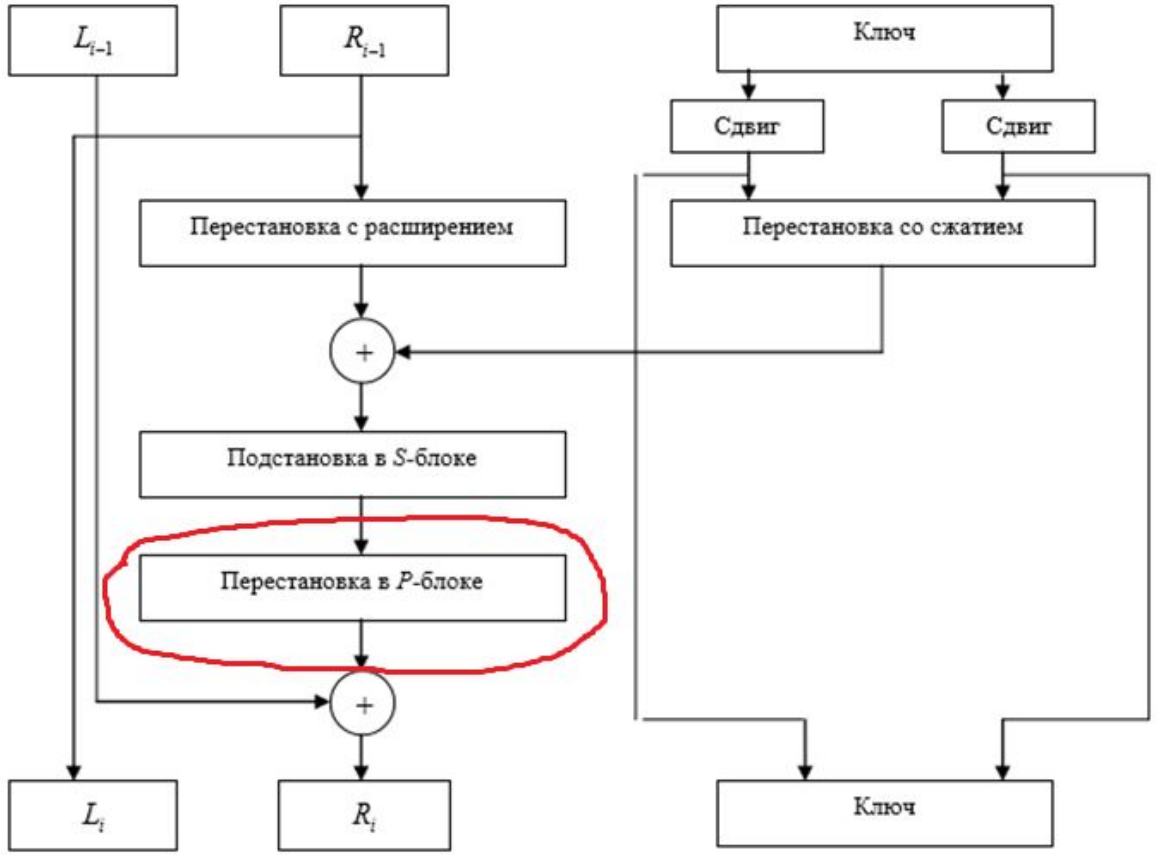
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13



Шифр DES. Раундовая функция шифрования.

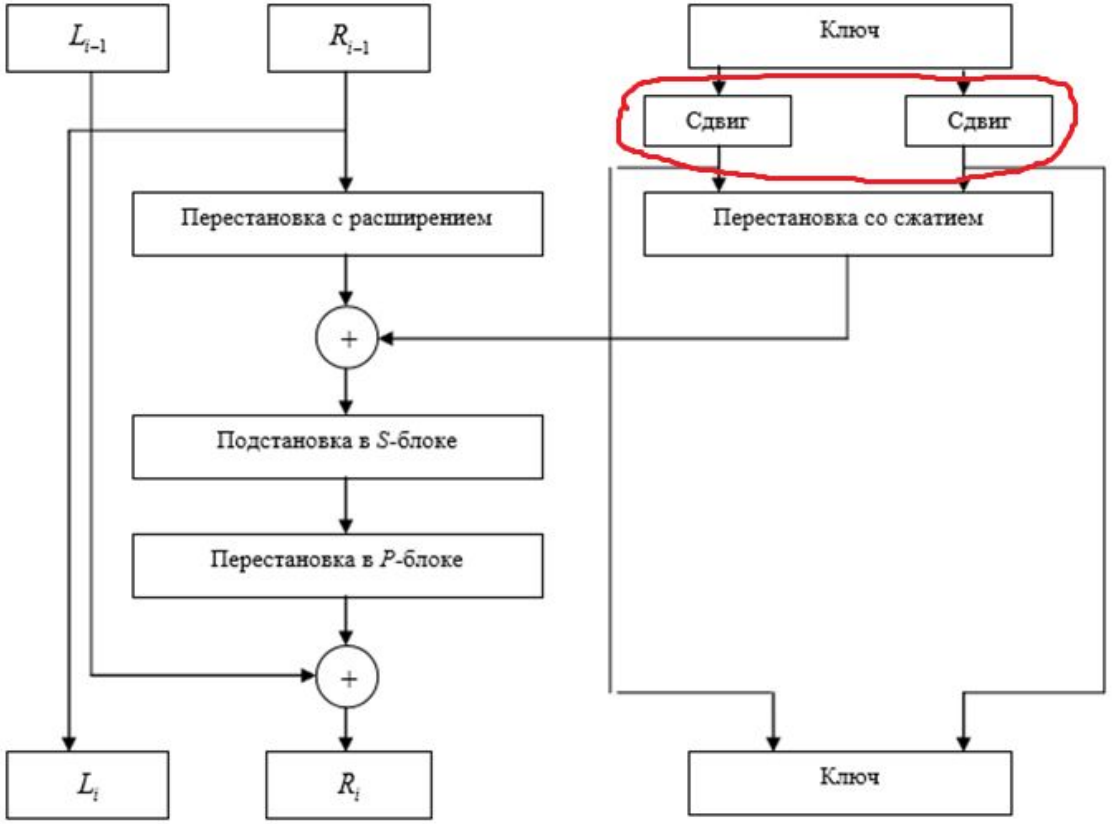
Результат подстановки в блоках замен S, состоящий из 32 бит, полученный в предыдущей операции, подвергается перестановке.

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



Шифр DES. Преобразование ключа.

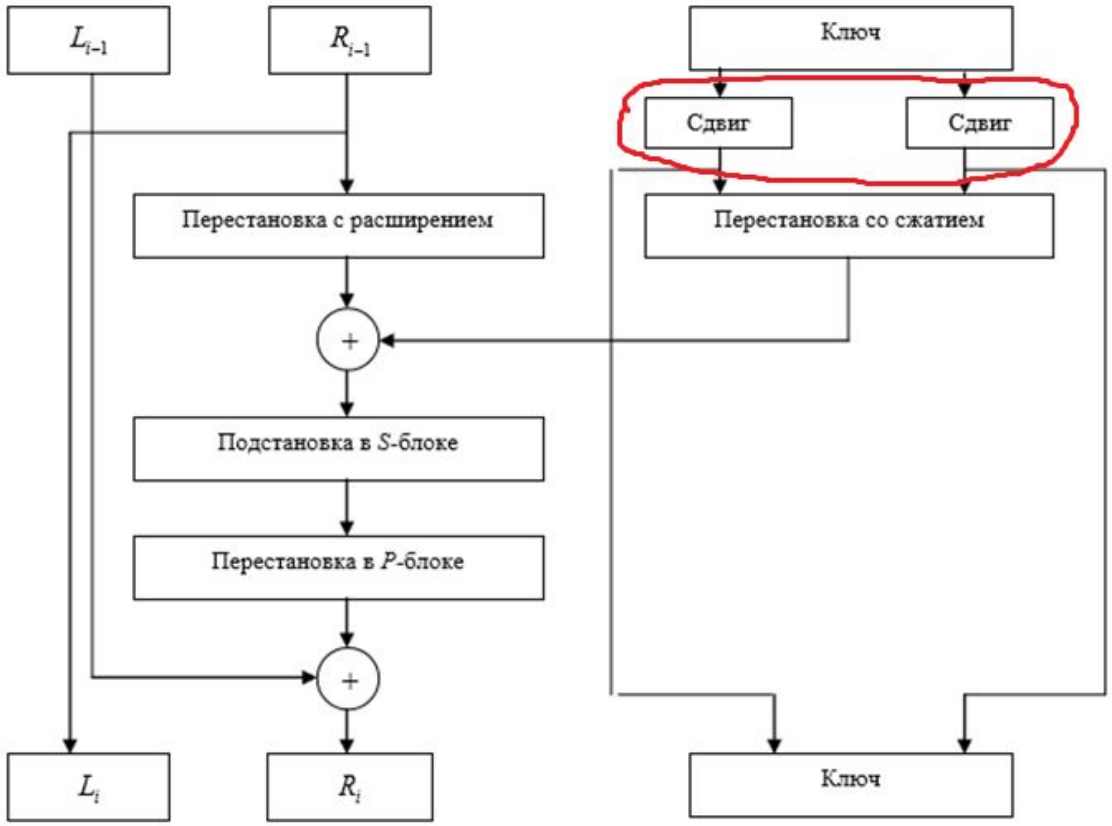
Ключевой массив в каждом раунде преобразовывается на основе циклического сдвига вправо. Число позиций сдвига в каждом раунде определяется массивом m из 16 элементов m = {0, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1}. Значение элемента в этом массиве соответствует числу позиций сдвига на каждом раунде шифрования. Сдвигается не весь массив, а половины.



Шифр DES. Преобразование ключа.

Далее производится перестановка со сжатием. Согласно этой таблице из 56 бит выбирается только 48 бит ключевого массива, причем 14 бит становится первым, 17 — вторым и т. д.

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



Шифр DES. Конечная перестановка.

Блок конечной таблицы перестановки бит. В соответствии с этой таблицей 40 бит текста становится первым битом, 8 бит становится вторым битом, 48 бит — третьим, а первый бит текста перемещается на 58 позицию и т. д.

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