

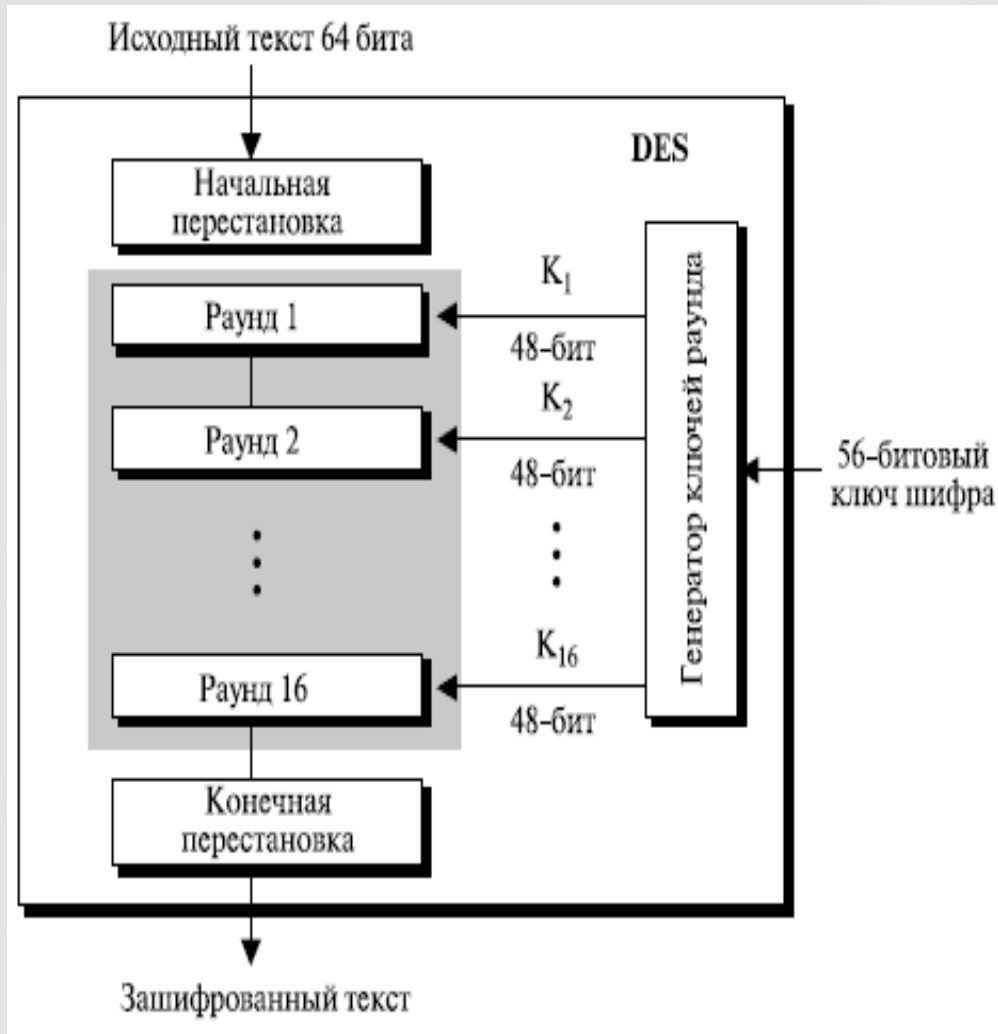
МЕТОДЫ СИММЕТРИЧНОГО ШИФРОВАНИЯ

Алгоритм стандарта шифрования DES (*Data Encryption Standard*)

Историческая справка о DES

- Стандарт шифрования данных (DES) — блочный шифр с симметричными ключами, разработан Национальным Институтом Стандартов и Технологии (*NIST – National Institute of Standards and Technology*).
- В 1973 году NIST издал запрос для разработки предложения национальной криптографической системы с симметричными ключами. Предложенная IBM модификация проекта, названного Lucifer, была принята как DES.
- DES был издан в марте 1975 года как Федеральный Стандарт Обработки Информации (*FIPS – Federal Information Processing Standard*).

Структура DES



- Открытый текст шифруется блоками 64 бит, используя 64 битный ключ шифра (56 битов фактический ключ+8 битов четности)
- Процесс шифрования состоит из двух перестановок (P-блоки) и 16-ти раундов Фейстеля
- Каждый раунд использует различные 48-битовые раундовые ключи, сгенерированный на основе ключа шифра
- Для шифрования и расшифрования используется один и тот же алгоритм и ключ

Начальная и конечная перестановки

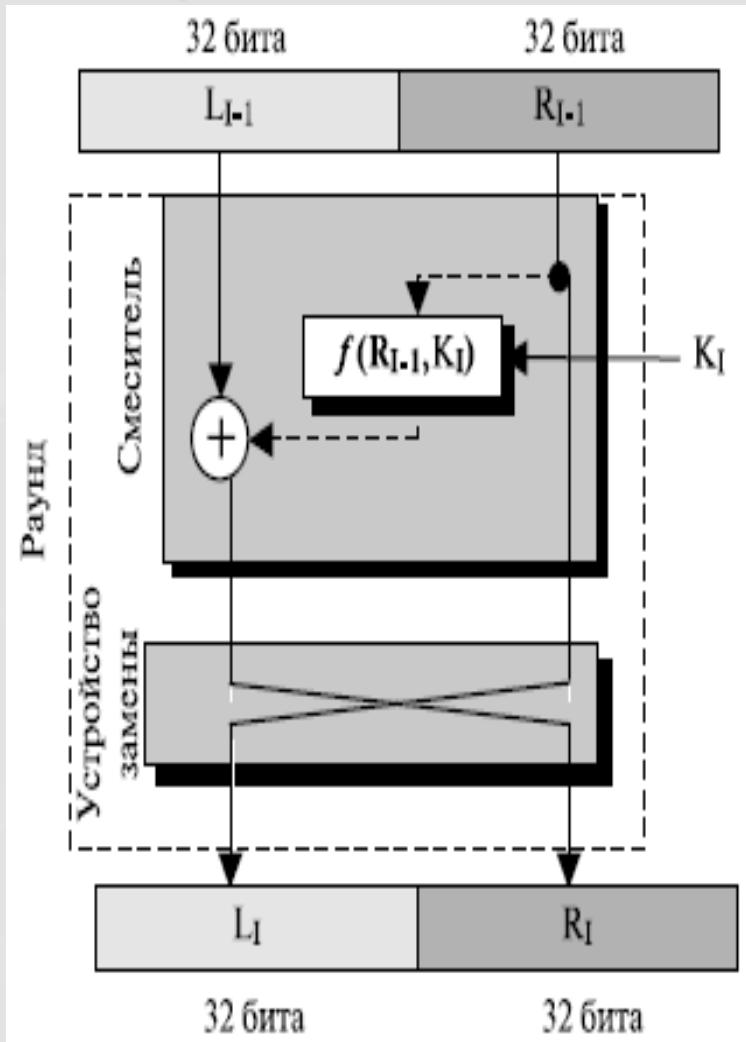
Прямая перестановка IP блока открытого текста

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

Обратная перестановка IP^{-1} блока шифротекста

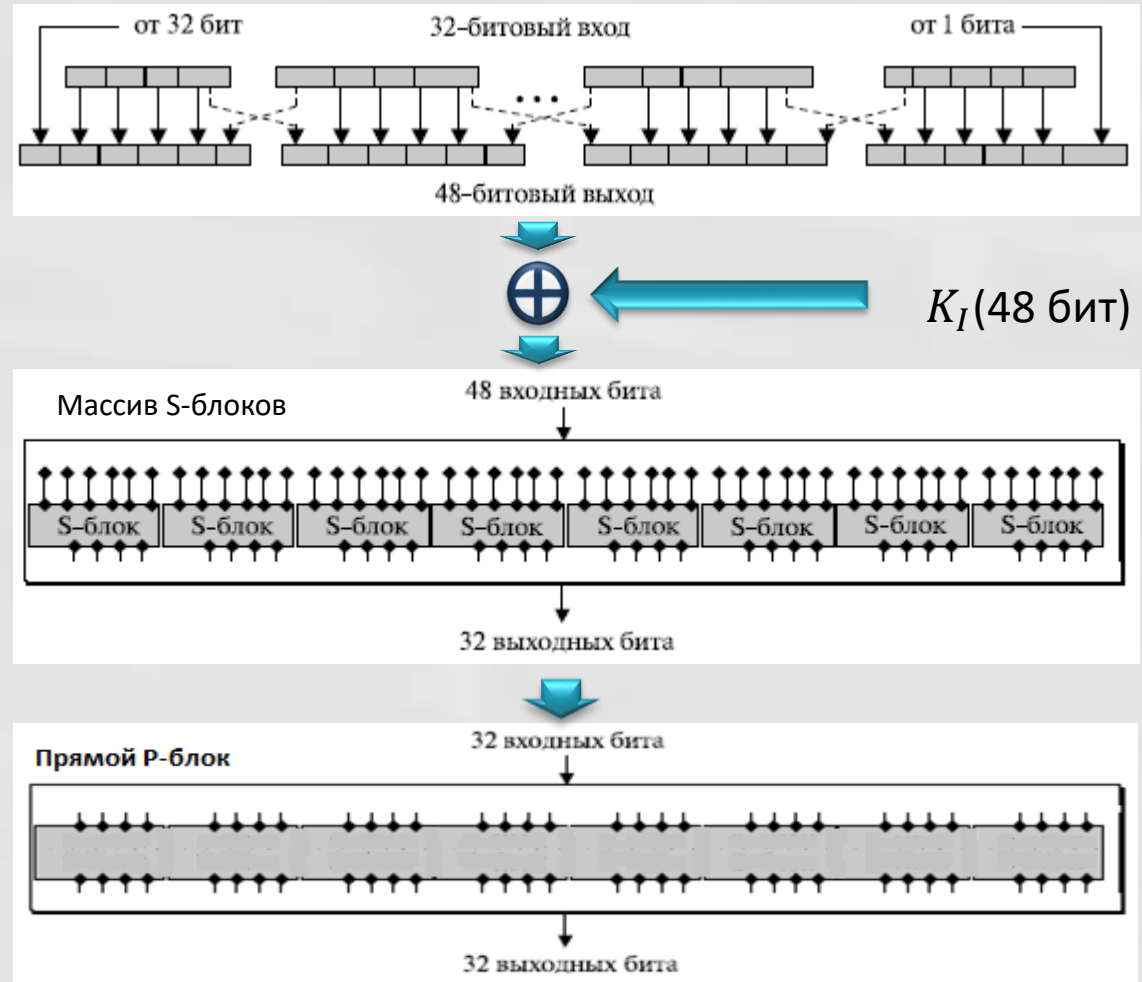
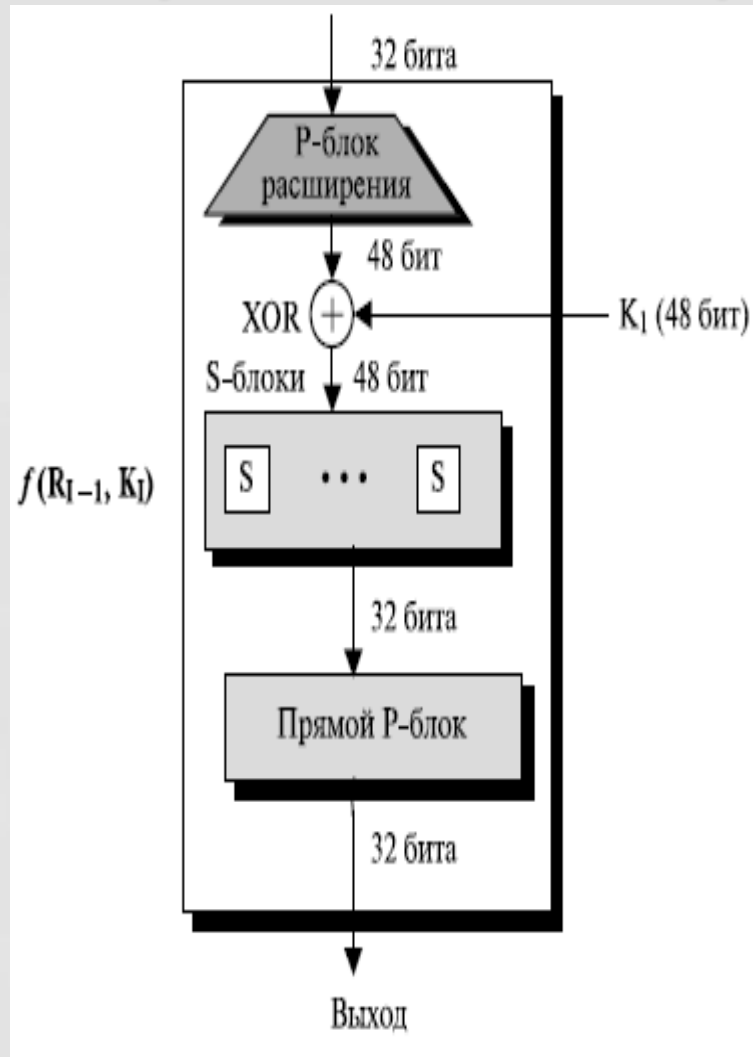
40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Раунды DES



- На входе раунда субблоки от предыдущего раунда
- Выполняется необратимое преобразование (функция DES) правого субблока
- Вычисляется XOR левого субблока и результата преобразования
- Субблоки меняются местами

Функция шифрования DES



Р-блоки перестановки

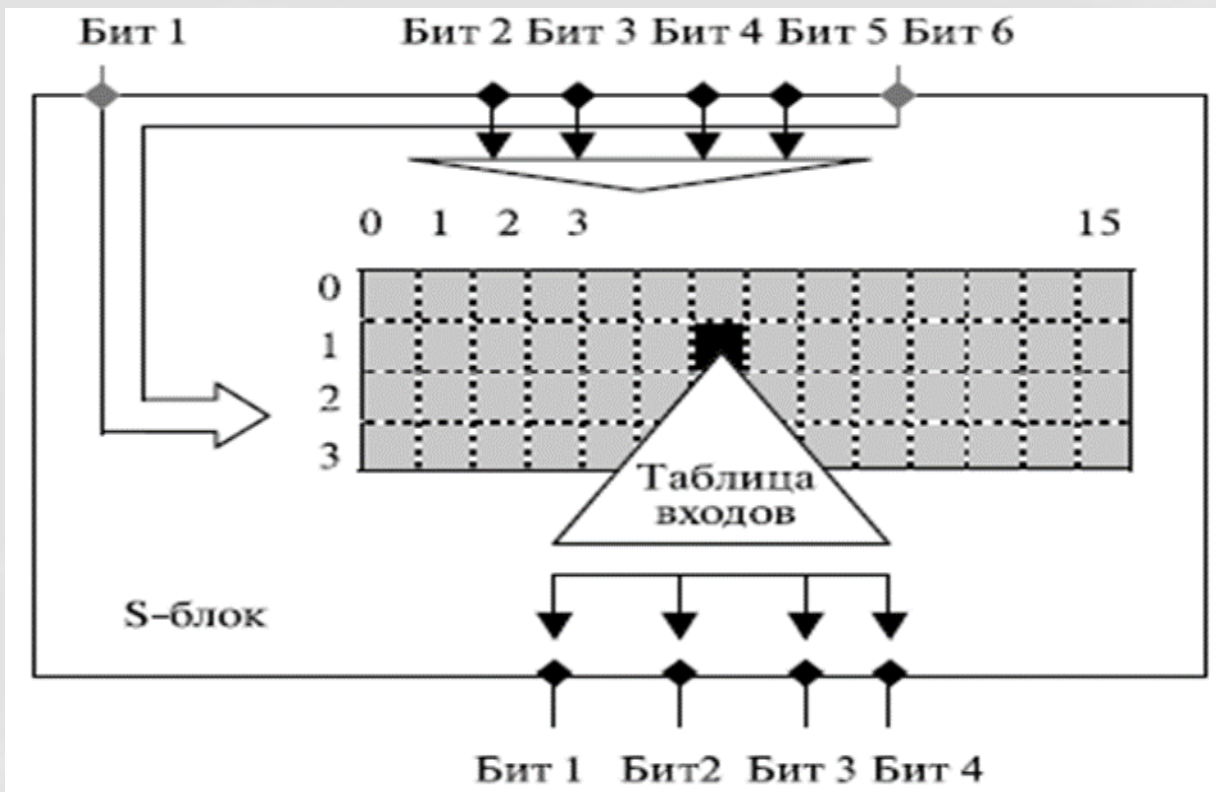
Р-блок расширения (переставляет биты субблока R_{I-1})

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

Прямой Р-блок (переставляет биты выходов S-блоков)

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

S-блоки функции DES



- Для каждого S-блока есть собственная таблица (всего 8)
- Комбинация битов 1 и 6 на входе определяет одну из четырех строк
- Комбинация битов от 2 -го до 5 -го определяет один из шестнадцати столбцов
- 4-х битовая подстановка берется из клетки на пересечении строки и столбца
- Пример: S-блок 1

1 0110 0

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	07	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	07	05	11	03	14	10	00	06	13	

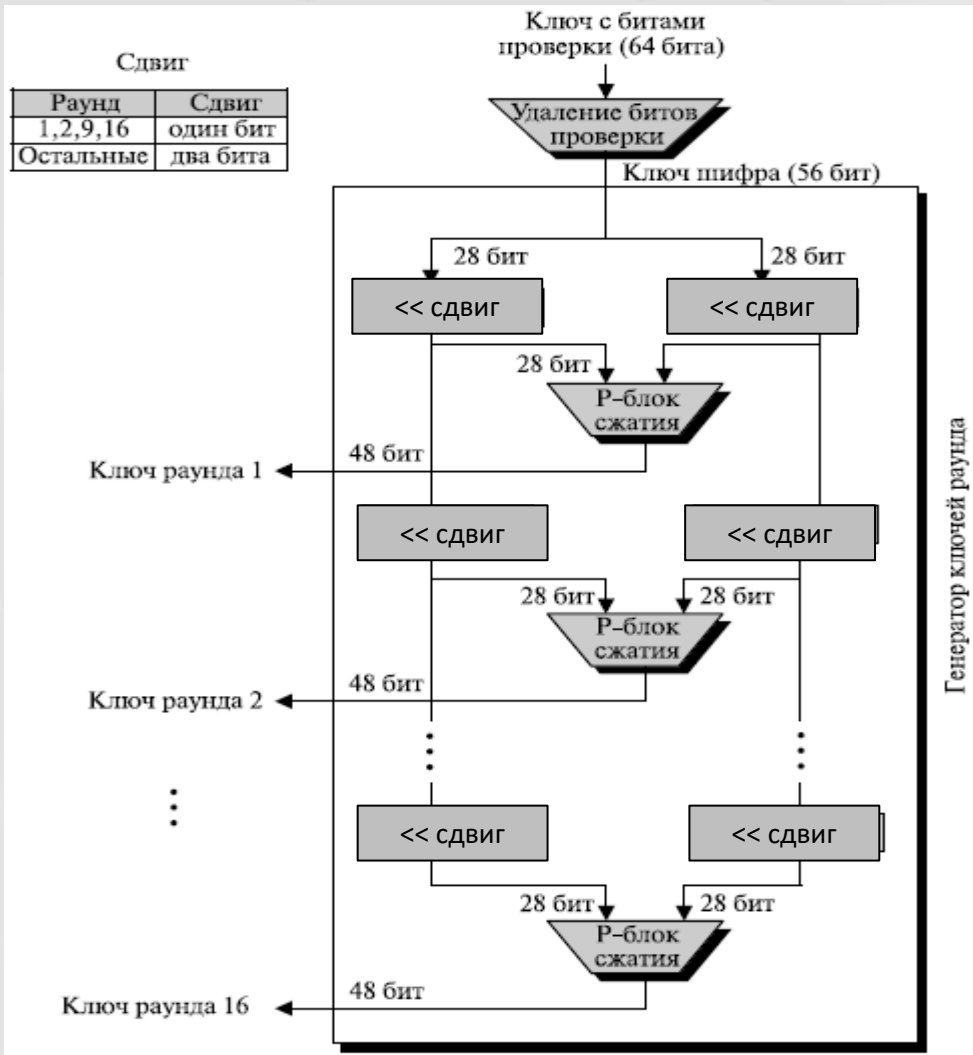
0010

Таблицы подстановок S-блоков

	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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_5
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_6
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_8
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_9
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	

Генерация раундовых ключей DES



- Удаляются биты проверки 8, 16, 32, ..., 64, ключ разделяется пополам и выполняется перестановка 56 бит фактического ключа

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

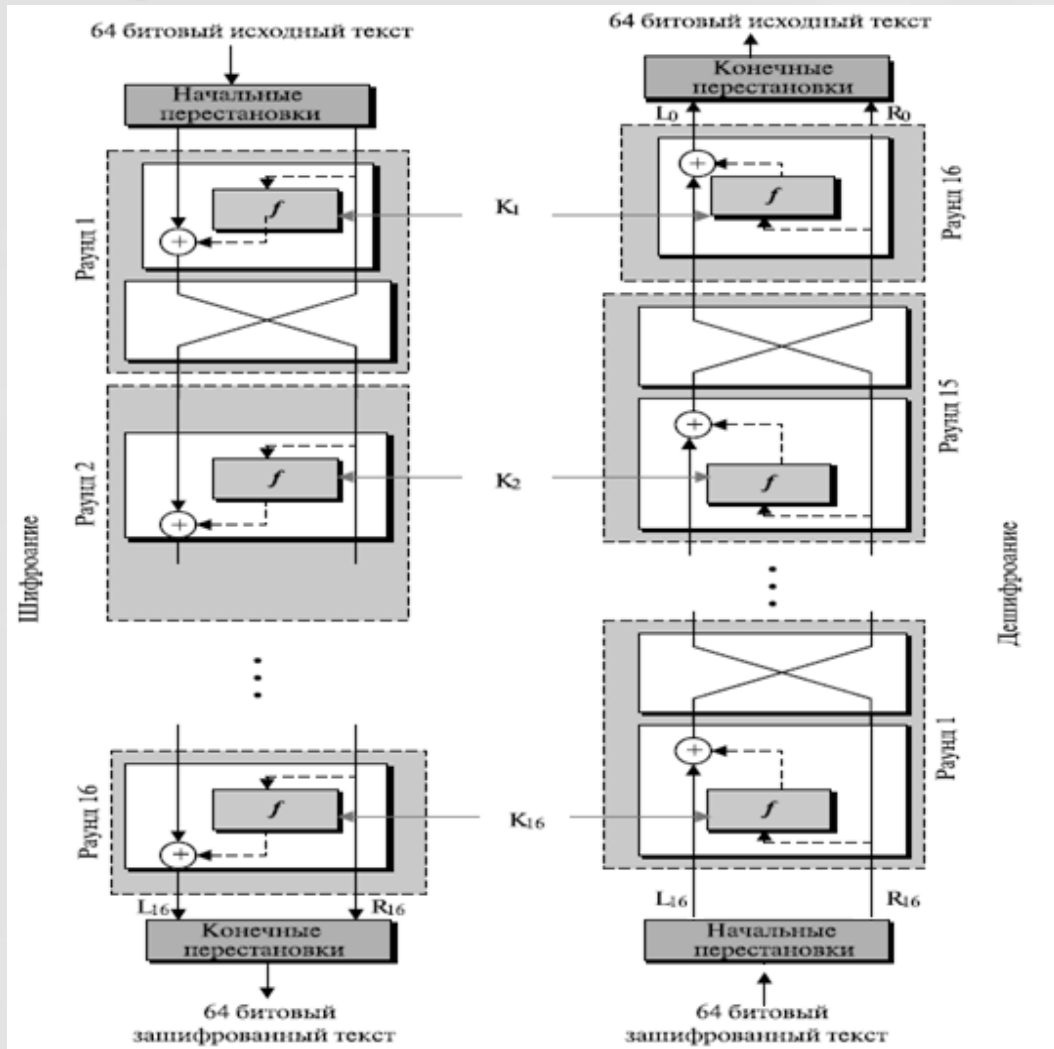
- Каждая половинка циклически сдвигается влево в зависимости от номера раунда

Раунд	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Число бит	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

- Половинки ключа объединяются и обрабатываются Р-блоком сжатия

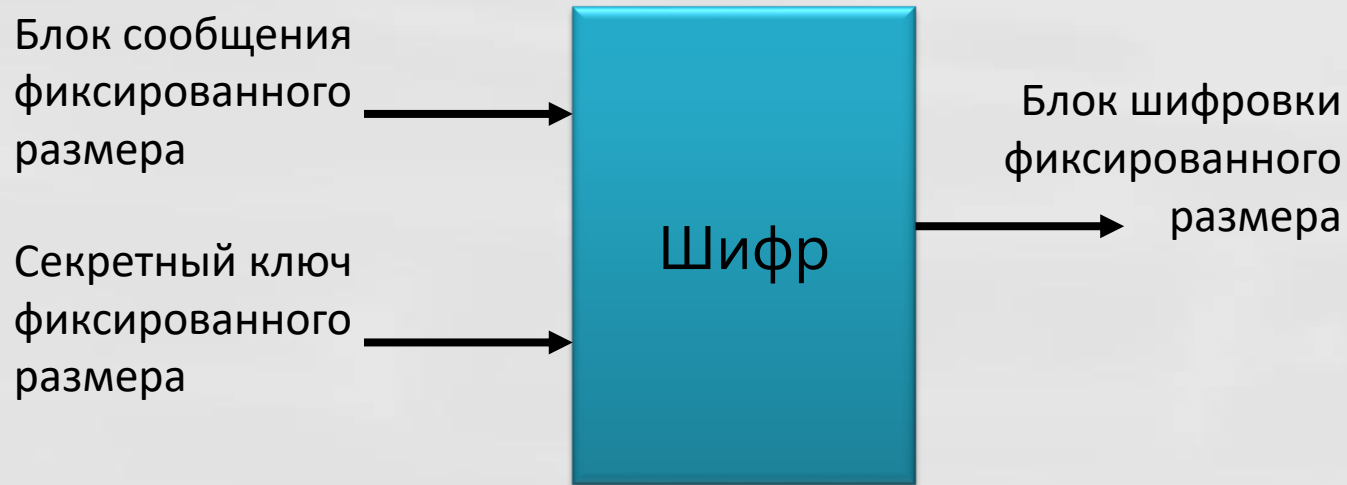
14	17	11	24	1	5	3	28	15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2	41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32

Обратимость DES



- Последний раунд отличается других: он содержать только смеситель и не содержит устройства замены
- Ключи раундов применяются при шифровании и дешифровании в обратном порядке

Спецификация симметричного блочного шифра



- Пример: Шифр DES:
 - Блок сообщения 64 бит
 - Секретный ключ 64 бит
 - Блок шифровки 64 бит

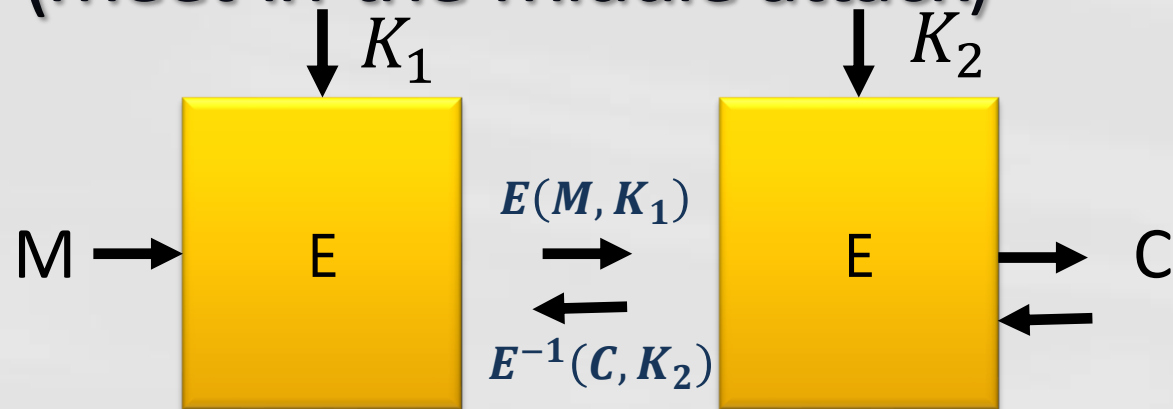
Проблемы DES

- Недостаточная длина ключа. Существует всего $2^{56} = 7,2 \cdot 10^{16}$ возможных ключей, что в настоящее время допускает успешное применение лобовых атак
- Проблемы с ключами шифрования:
 - 4 ключа являются слабыми (порождают одинаковые раундовые ключи). Это ключи, в которых все биты какой-либо из половин расширяемого ключа являются нулевыми или единичными.
 - 6 пар ключей являются эквивалентными (т.е. информация, зашифрованная одним ключом из пары, расшифровывается другим ключом той же пары).
 - 48 ключей являются «возможно слабыми», Возможно слабые ключи при их расширении дают только 4 различных ключа раунда
- Существует опасность, что эти S-блоки (основа алгоритма) конструировались таким образом, чтобы был возможен криптоанализ со стороны разработчика, который знает их слабые стороны (пока нет подтверждений)

Взлом DES

- 1998 г. используя суперкомпьютер стоимостью 250 тыс. долл., сотрудники RSA Laboratory «взломали» DES менее чем за три дня. Эксперимент проходил в рамках исследования DES Challenge II, проводимого RSA Laboratory под руководством общественной организации Electronic Frontier Foundation (EFF). Суперкомпьютер, построенный в RSA Laboratory для расшифровки данных, закодированных методом DES по 56-разрядному ключу, получил название EFF DES Cracker.

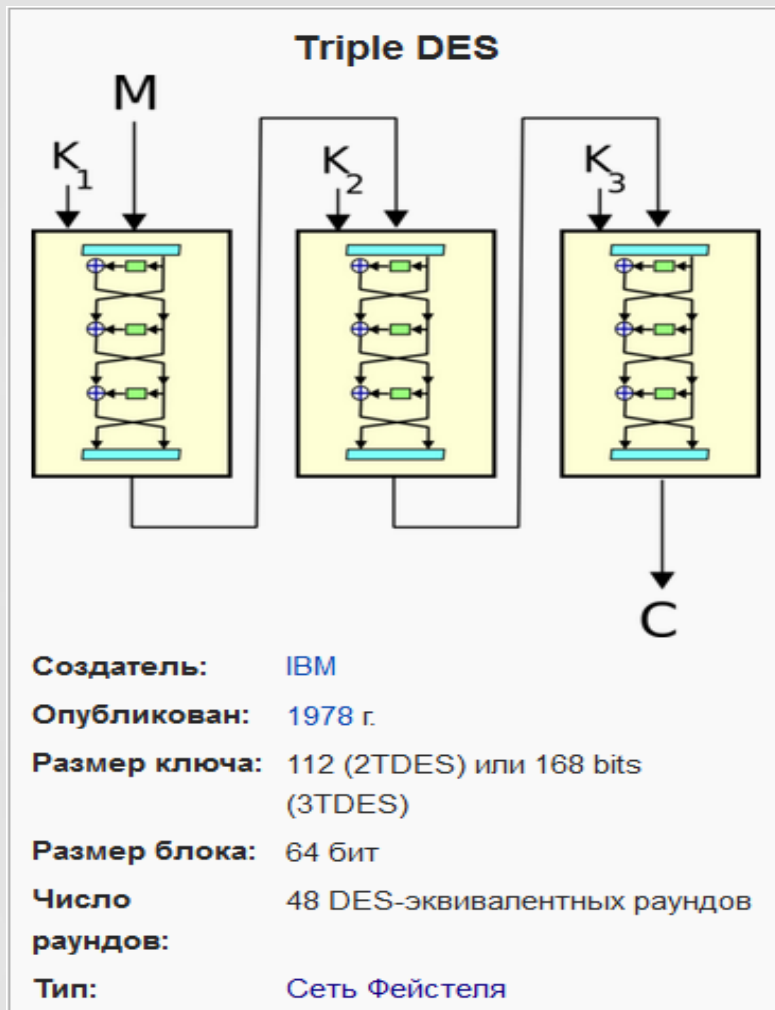
Шифр Double DES и атака встреча посередине (meet-in-the-middle attack)



$$C = E(E(M, K_1), K_2)$$
$$M = E^{-1}(E^{-1}(C, K_2), K_1)$$

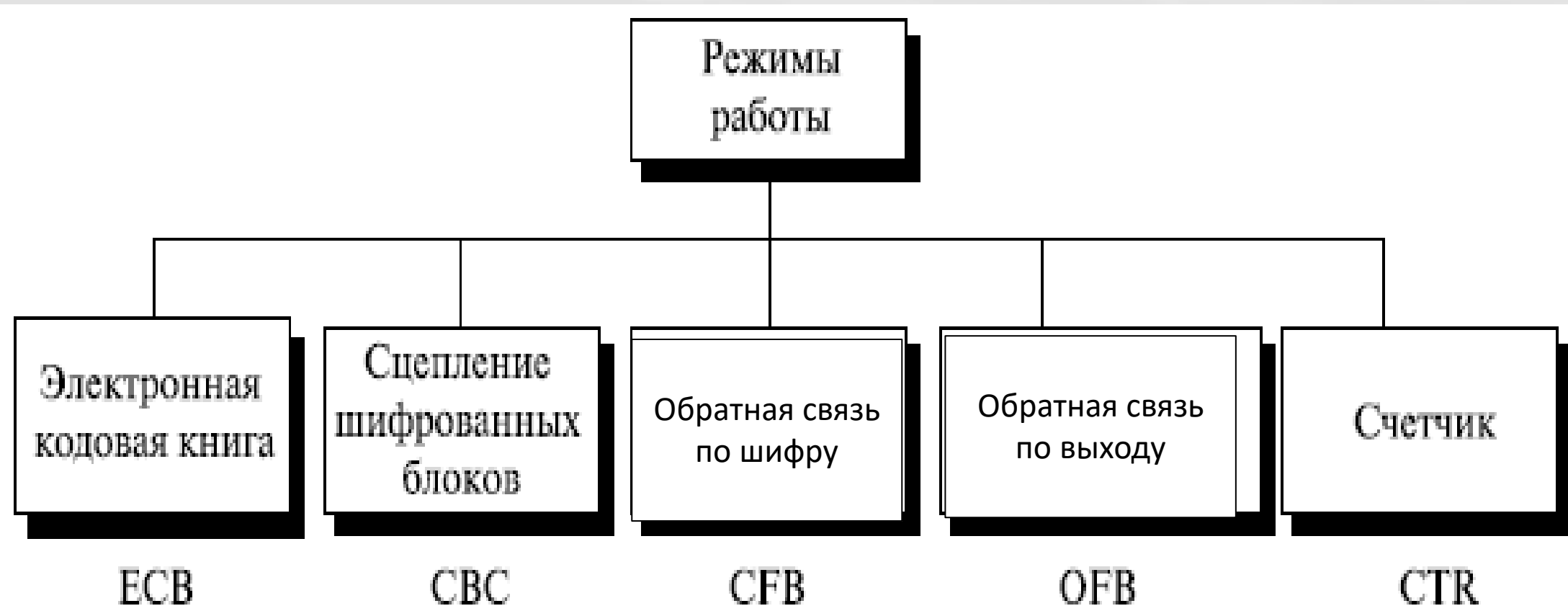
- Ищем такую пару K_1 и K_2 , чтобы $E(M, K_1) = E^{-1}(C, K_2)$
- Сложность атаки (меньше ожидаемой $\sim 2^{112}$)
 - 2^{56} шифрований и $\sim 2^{56}$ ячеек памяти для хранения вариантов K_1
 - 2^{56} расшифрований $\sim 2^{56}$ ячеек памяти для хранения вариантов K_2

Шифр Triple DES

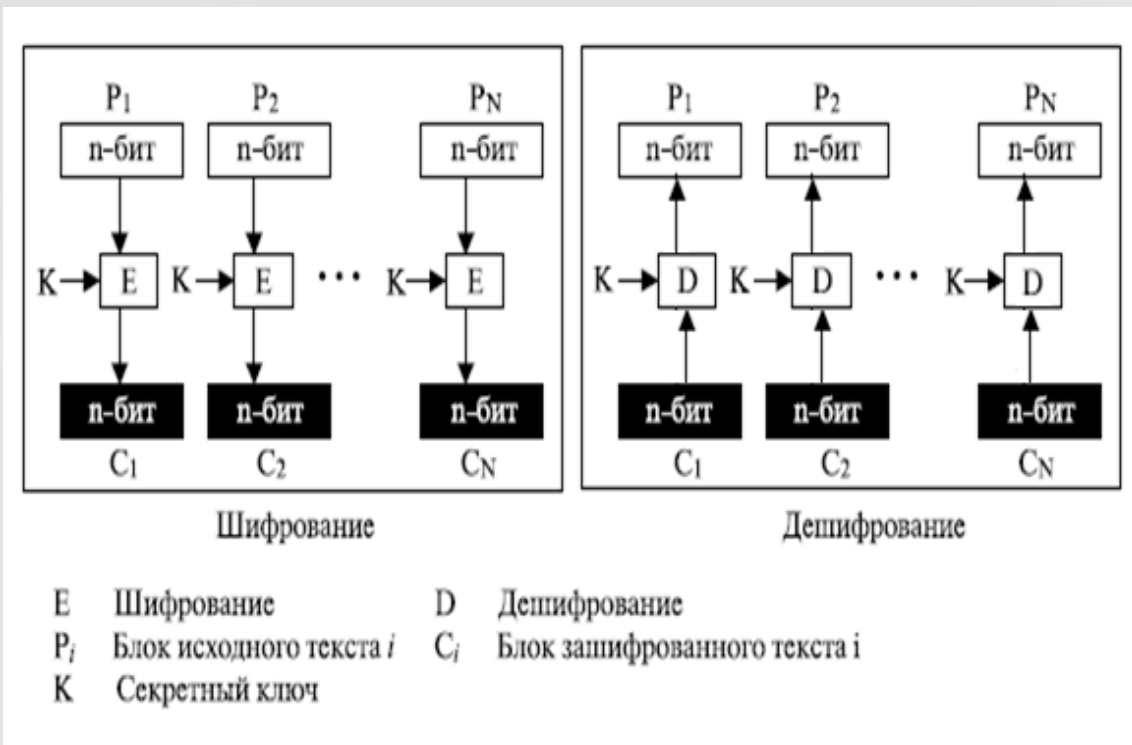


- Модификации:
 - DES-EEE3
 - DES-EDE3
 - DES-EEE2
 - DES-EDE2
- Самая популярная разновидность это DES-EDE3 и DES-EDE2
- Реализован во многих приложениях, ориентированных на работу с Интернет, в том числе в PGP и S/mime.

Режимы работы блочных шифров



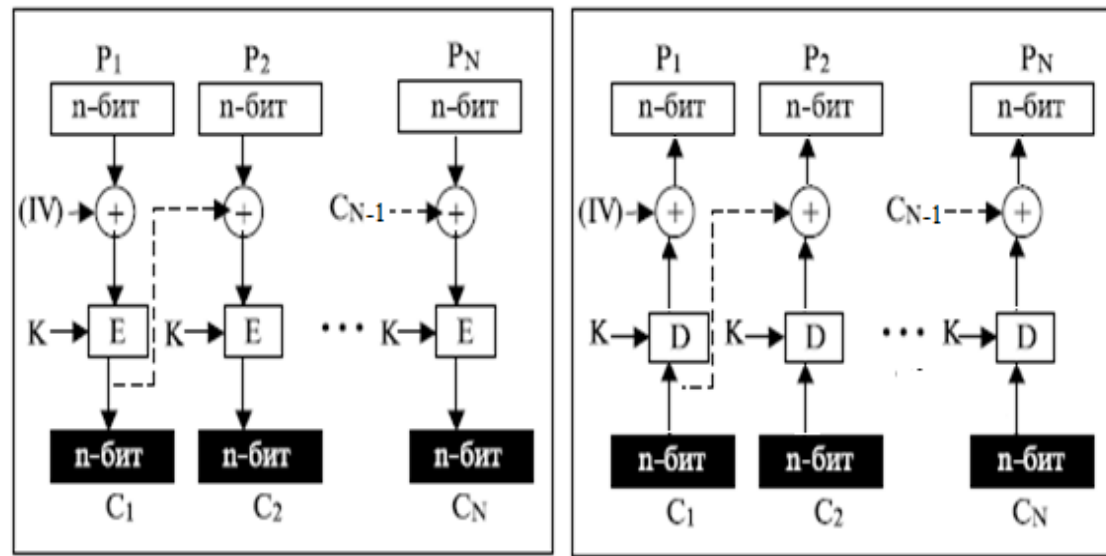
Режим электронной кодовой книги



ECB — Electronic Code Book

- **Достоинства:**
 - Шифрование может быть параллельным
 - Ошибка в передаче блока не имеет никакого воздействия на другие блоки
- **Недостатки:**
 - Одинаковые блоки открытого текста будут преобразовываться в одинаковые блоки шифротекста
 - Независимость блоков создает возможность для замены некоторых блоков зашифрованного текста без знания ключа

Режим сцепления блоков шифротекста



Шифрование

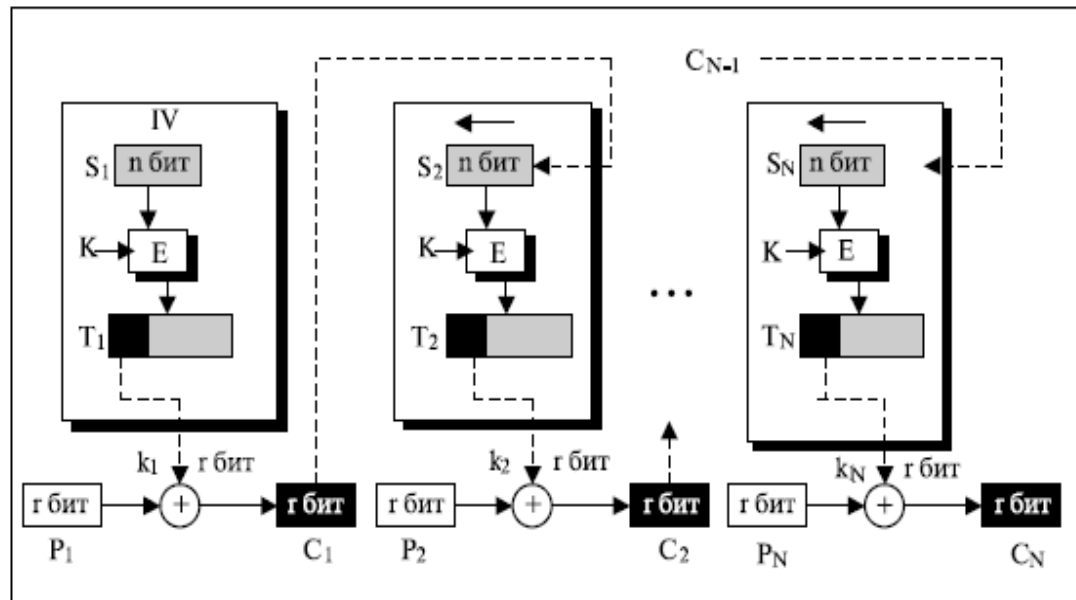
Дешифрование

E Шифрование D Дешифрование
 P_i Блок исходного текста i C_i Блок зашифрованного текста i
 K Секретный ключ

- Достоинства:
 - Одинаковые блоки исходного текста, преобразуются в различные блоки шифротекста.
 - Если произойдёт изменение одного бита шифротекста, то данная ошибка распространится на следующие блоки, но при расшифровке произойдет самовосстановление
 - Последний блок шифротекста зависит от всех бит отrypted текста сообщения и может использоваться для контроля целостности сообщения
- Недостатки:
 - Зашифрование сообщения не поддаётся распараллеливанию

CBC — Cipher Block Chaining
IV - Initialization Vector

Режим обратной связи по шифру



Е: Шифрование
 P_j : Блок исходного текста
К: Секретный ключ
D: Дешифрование
 C_j : Блок зашифрованного текста
IV: Начальный вектор (S_1)
 S_j : Регистр сдвига
 T_j : Временный регистр

CFB - Cipher Feedback

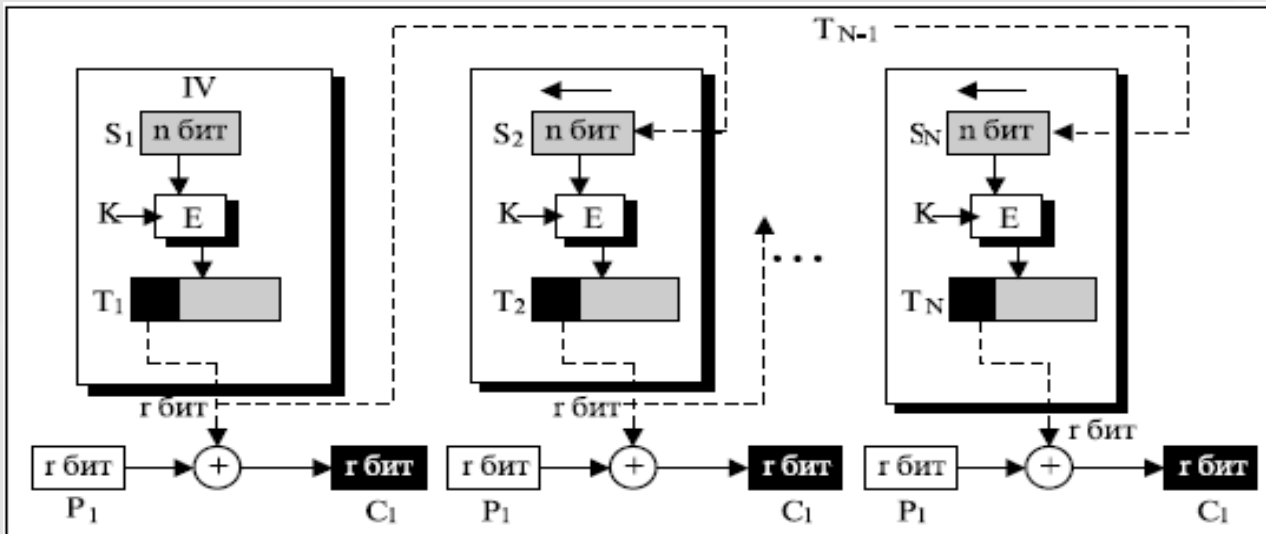
Достоинства:

- Это шифр потока, в котором ключевой поток зависит от зашифрованного текста
- В этом режиме не требуется дополнение блоков,

Недостатки:

- Ошибка в единственном бите шифротекста создает ошибку в следующих блоках до тех пор, пока, ошибка находится в регистре сдвига

Режим обратной связи по выходу



Шифрование

E:	Шифрование	D:	Дешифрование
P_i :	Блок i исходного текста	C_i :	Блок i зашифрованного текста
K:	Секретный ключ	IV:	Начальный вектор (S_1)
S_i :	Регистр сдвига	T_i :	Временный регистр

Достоинства:

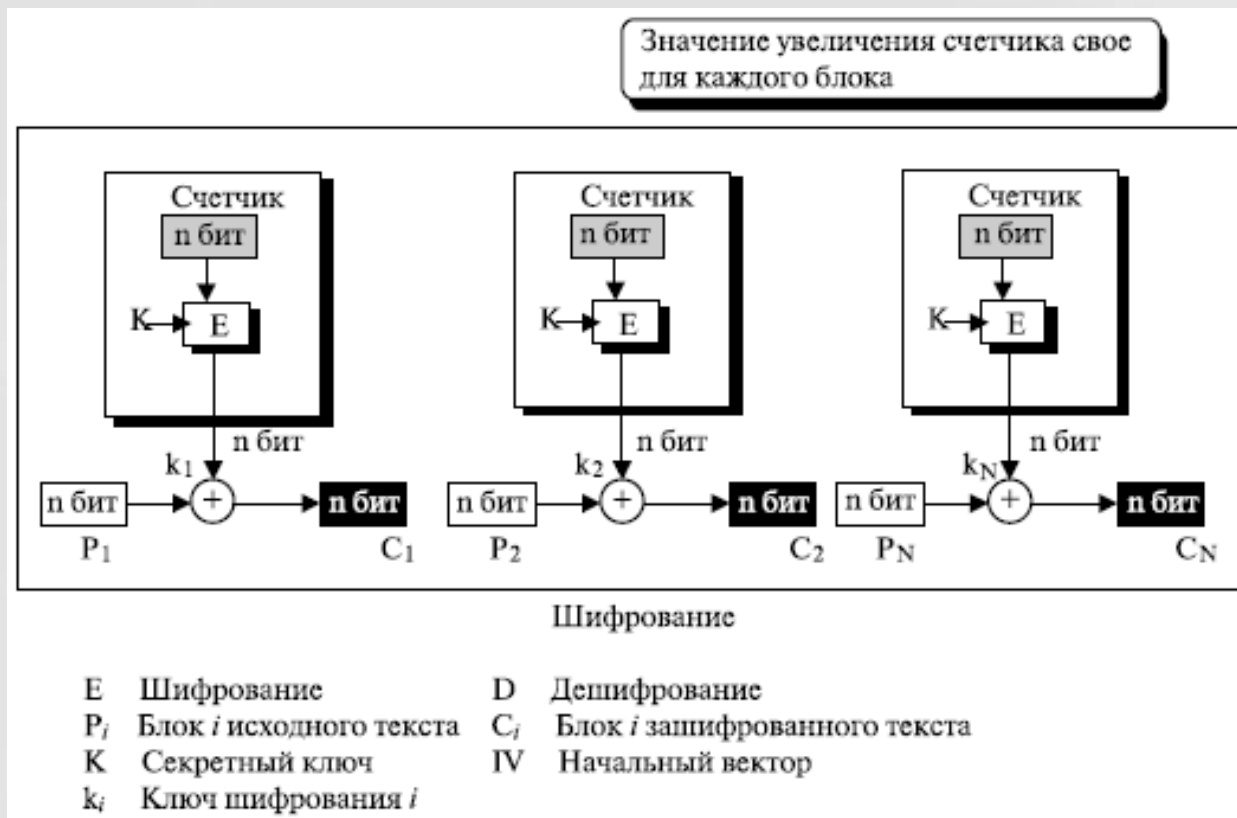
- Фактически, это шифр потока, в котором ключевой поток не зависит от исходного и зашифрованного текста
- Каждый бит в зашифрованном тексте независим от предыдущего бита или битов. Это позволяет избежать распространения ошибок

Недостатки:

- Чтобы одним и тем же ключом зашифровать больше, чем одно сообщение, значение IV должно быть изменено для каждого сообщения

OFB - Output Feedback

Режим счетчика



CTR - Counter

Достоинства:

- Создает n -битовый зашифрованный текст, блоки которого независимы друг от друга — они зависят только от значений счетчика. Фактически, это шифр потока
- Режим, подобно режиму ECB, может использоваться, чтобы зашифровать и расшифровывать файлы произвольного доступа, и значение счетчика может быть связано номером записи в файле

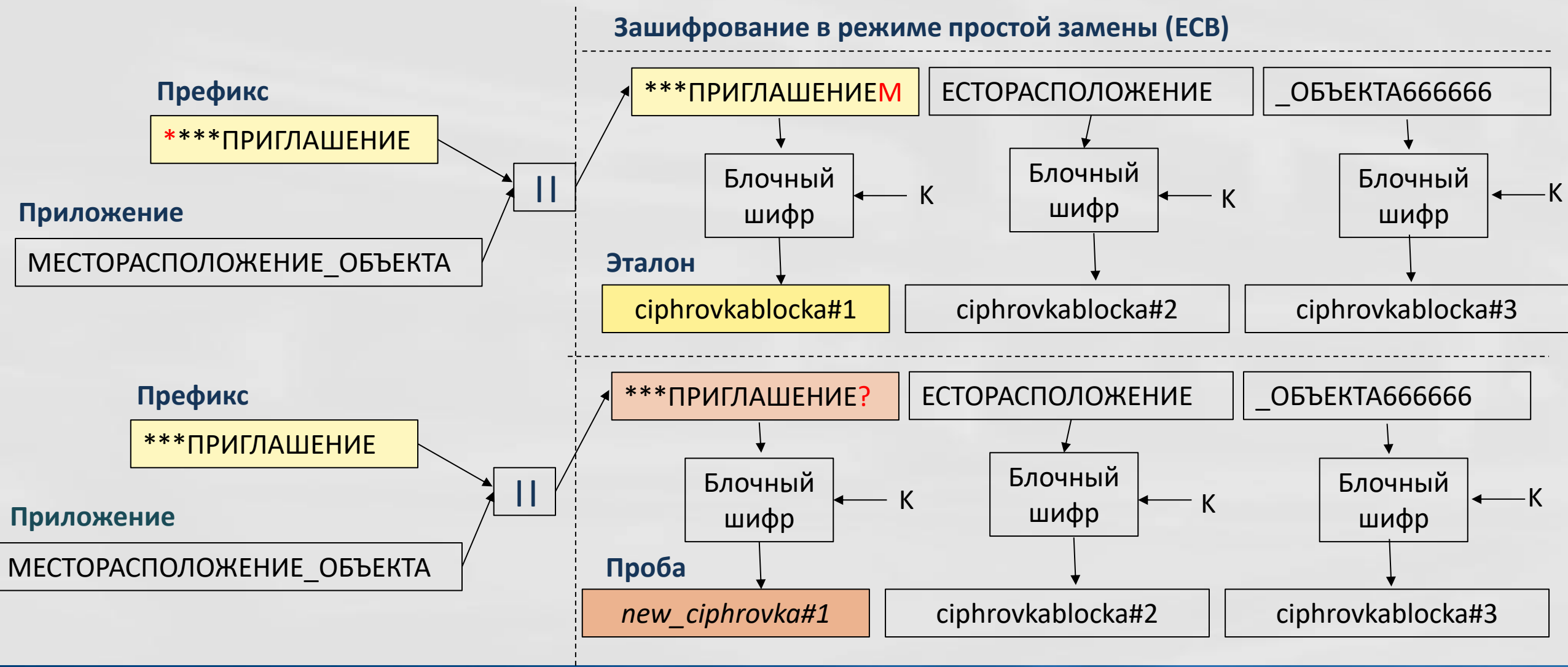
Недостатки:

- Если значения счетчиков совпадает, то шифрование производится на одном ключе

Атака с выбранным открытым текстом на режим ECB

- Цель: дешифровать конфиденциальную часть открытого текста без знания ключа
- Модель нарушителя:
 - Знает используемый режим работы блочного шифра, длину блока и способ дополнения последнего блока
 - Умеет формировать и добавлять префикс к конфиденциальной (для нарушителя) части открытого текста и делать это незаметно и многократно
 - Умеет перехватывать шифровку всего сообщения и разделять ее на блоки и сохранять копии необходимых блоков

Тактика действий нарушителя (ЕСВ)



МЕТОДЫ СИММЕТРИЧНОГО ШИФРОВАНИЯ

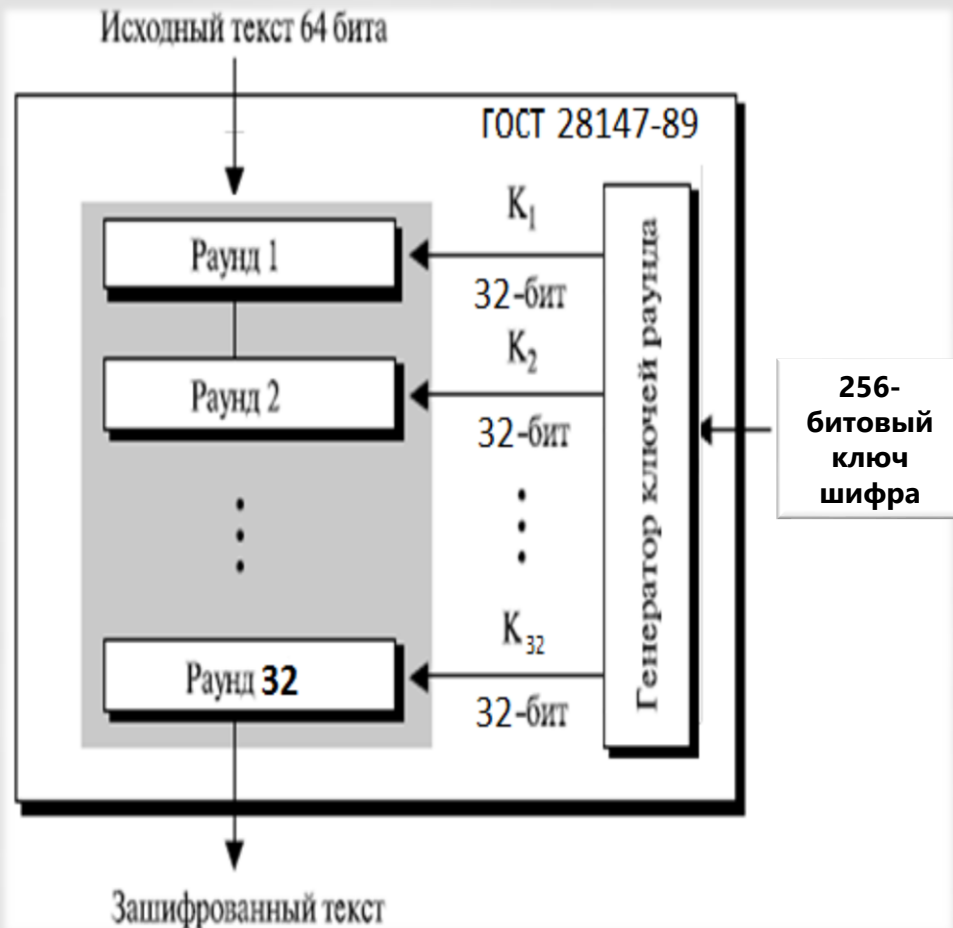
Магма - алгоритм стандартов шифрования
ГОСТ 28147-89, ГОСТ Р 34.12–2015, ГОСТ 34.12–2018



Историческая справка

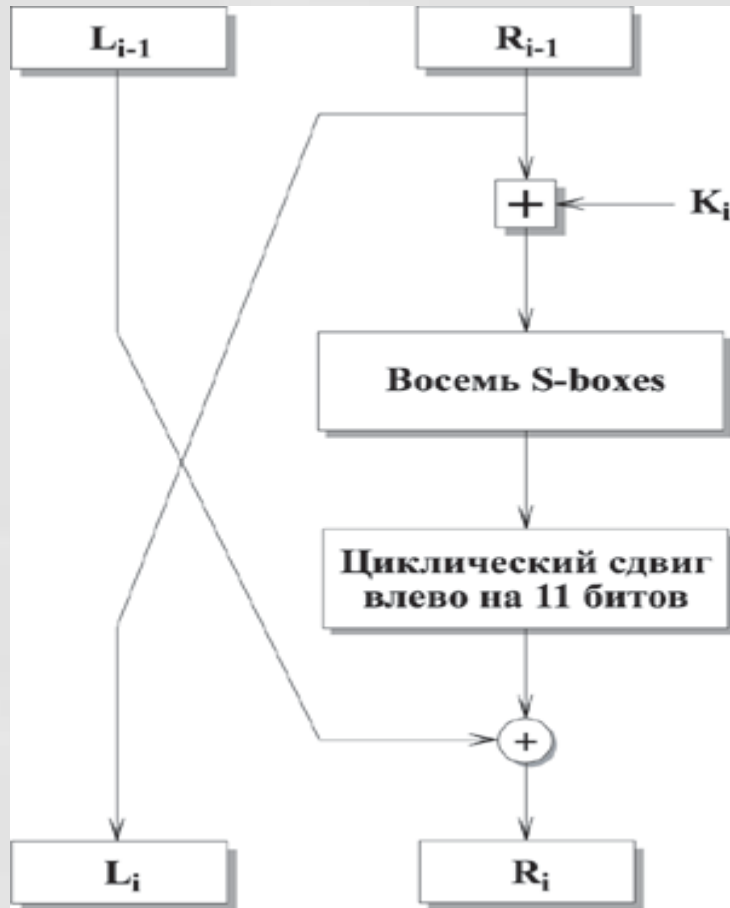
- **ГОСТ 28147—89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.** Советский и российский стандарт симметричного шифрования, введённый в 1990 году. По некоторым сведениям, алгоритм, положенный впоследствии в основу стандарта, родился, предположительно в 1970-х годах. С момента опубликования этого ГОСТа на нём стоял ограничительный гриф «Для служебного пользования», и формально шифр был объявлен полностью открытым» только в мае 1994 года.
- **ГОСТ 3412-2015 Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Блочные шифры.** Ввел в действие в июне 2015 сразу два блочных шифра , на которые разрешено ссылаться «Магма» (аналог ГОСТ 28147—89) и «Кузнечик»
- **ГОСТ 34.12-2018 – Информационная технология. Криптографическая защита информации . Блочные шифры.** Введен в действие в ноябре 2018 терминологическая и концептуальная увязка с международными стандартами от ИСО

Структура шифра «Магма»



- Открытый текст шифруется блоками 64 бит, используя 256 битный ключ шифра
- Процесс шифрования состоит из 32-х раундов схемы Фейстеля и назван *базовым циклом зашифрования (32-3)*
- Каждый раунд использует 32 -битовый раундовый ключ (*элемент ключа* шифрования), сгенерированный на основе ключа шифра
- Для расшифрования используется тот же алгоритм и ключ
- Процесс расшифрования назван *базовым циклом расшифровывания (32-P)*
- Еще есть *базовый цикл выработки имитовставки (16-3)*

Раунды шифра «Магма»



- Раунд назван *основным шагом криптопреобразования*
- На входе раунда субблоки от предыдущего раунда
- В левый субблок копируется содержимое правого субблока
- Правый субблок и раундовый ключ складываются по модулю 2^{32}
- Результат сложения разбивается на восемь 4-битных значений (*блоков кода*), каждое из которых подается для замены на вход S-блока (*узла таблицы замен*)
- Выходы всех S-блоков объединяются в 32-битное слово, которое затем циклически сдвигается на 11 бит влево
- Вычисляется XOR результата с левым субблоком и результат обновляет правый субблок

S-блоки в шифре «Магма»

Номер S- блока	Подстановка															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	12	4	6	2	10	5	11	9	14	8	13	7	0	3	15	1
2	6	8	2	3	9	10	5	12	1	14	4	7	11	13	0	15
3	11	3	5	8	2	15	10	13	14	1	7	4	12	9	6	0
4	12	8	2	1	13	4	15	6	7	0	10	5	3	14	9	11
5	7	15	5	10	8	1	6	13	0	9	3	14	11	4	2	12
6	5	13	15	6	9	2	12	10	11	7	8	1	4	3	14	0
7	8	14	2	5	6	9	1	12	15	4	11	0	13	10	3	7
8	1	7	14	13	0	5	8	3	4	15	10	6	9	12	11	2

Алгоритм развертывания ключа в «Магме»

Раунд	1	2	3	4	5	6	7	8
Ключ	1	2	3	4	5	6	7	8
Раунд	9	10	11	12	13	14	15	16
Ключ	1	2	3	4	5	6	7	8
Раунд	17	18	19	20	21	22	23	24
Ключ	1	2	3	4	5	6	7	8
Раунд	25	26	27	28	29	30	31	32
Ключ	8	7	6	5	4	3	2	1

Схема использования раундовых ключей

- 256-битный ключ шифра последовательно разбивается на восемь 32-битных раундовых ключей
- Каждый раундовый ключ используется в четырех различных раундах по определенной схеме

Криптоанализ шифра «Магма»

- XSL-атака (eXtended Sparse Linearization) – метод, основанный на алгебраических свойствах шифра, предполагает решение особой системы уравнений.
- На первом этапе из достаточно большого количества пар открытых-шифрованных текстов выбирается те, которые позволяют рассматривать преобразования на меньшем, чем 32 количестве раундов
- На втором этапе результаты работы S-блоков описываются уравнениями вида:

$$\sum_{i,j} \alpha_{ij} * x_i * x_j + \sum_{i,j} \beta_{ij} * y_i * y_j + \sum_{i,j} \gamma_{ij} * x_i * y_j + \sum_i \delta_i * x_i + \sum_i \epsilon_i * y_i + \eta = 0$$

Где x_i и y_i – соответственно биты на входе и выходе S-блоков i -го раунда шифрования.

- Практический результат : 2^{64} известных открытых текста и $\sim 2^{64}$ бит памяти для хранения пар "открытый текст/шифртекст" позволяют взломать ГОСТ в 2^8 быстрее, чем простой перебор.

Сравнительный анализ «Магма» и DES

- В ГОСТ применяется 256-битный ключ шифра, а в DES 56-битный . При выборе сильных S-блоков ГОСТ считается очень стойким алгоритмом.
- В DES применяются нерегулярные перестановки P, в ГОСТ используется 11-битный циклический сдвиг влево. Поэтому ГОСТ требуется 8 раундов прежде, чем изменение одного входного бита повлияет на каждый бит результата; DES для этого нужно только 5 раундов.
- В DES только 16 раундов, в ГОСТ - 32 раунда, что делает его более стойким к дифференциальному и линейному криптоанализу
- ГОСТ использует гораздо более простую процедуру создания раундовых ключей, чем DES