Симметричное шифрование

Определение

Способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом шифрования являлось симметричное шифрование.

Виды симметричных шифров

- Блочные шифры – исходные данные разбиваются на блоки фиксированной длинны(например популярны длины в 64 или 128 бит), эти блоки шифруются поочерёдно, в зависимости от режима шифрования, могут шифроваться независимо друг от друга или со сцеплением.
- Поточные шифры – побитное или посимвольное шифрование данных

Виды симметричных шифров

- Часто процесс шифрования или расшифровывания представляется следующей абстрактной записью

$$C = E_{k1}(M)$$

$$M' = D_{k2}(C)$$

Где M(message)-исходное сообщение, C(cipher text) – шифртекст, E(encryption)-шифрующая ф-я, k1(key №1)

k2(key №2)-первый для зашифровывания и второй для расшифровывания ключи, M'-сообщение получаемое при расшифровывании, D(decryption)-функция расшифровывания

Две задачи Шеннона

- Рассеивание – малейшее изменение открытого текста приводит к значительному изменению шифр текста. свойство рассеивания принято называть лавинным эффектом.

- Полнота – зависимость всех битов шифртекста от каждого бита входного текста.

Необратимость

- В современных алгоритмах шифрования широко используются вычислительно необратимые функции

01011010 key

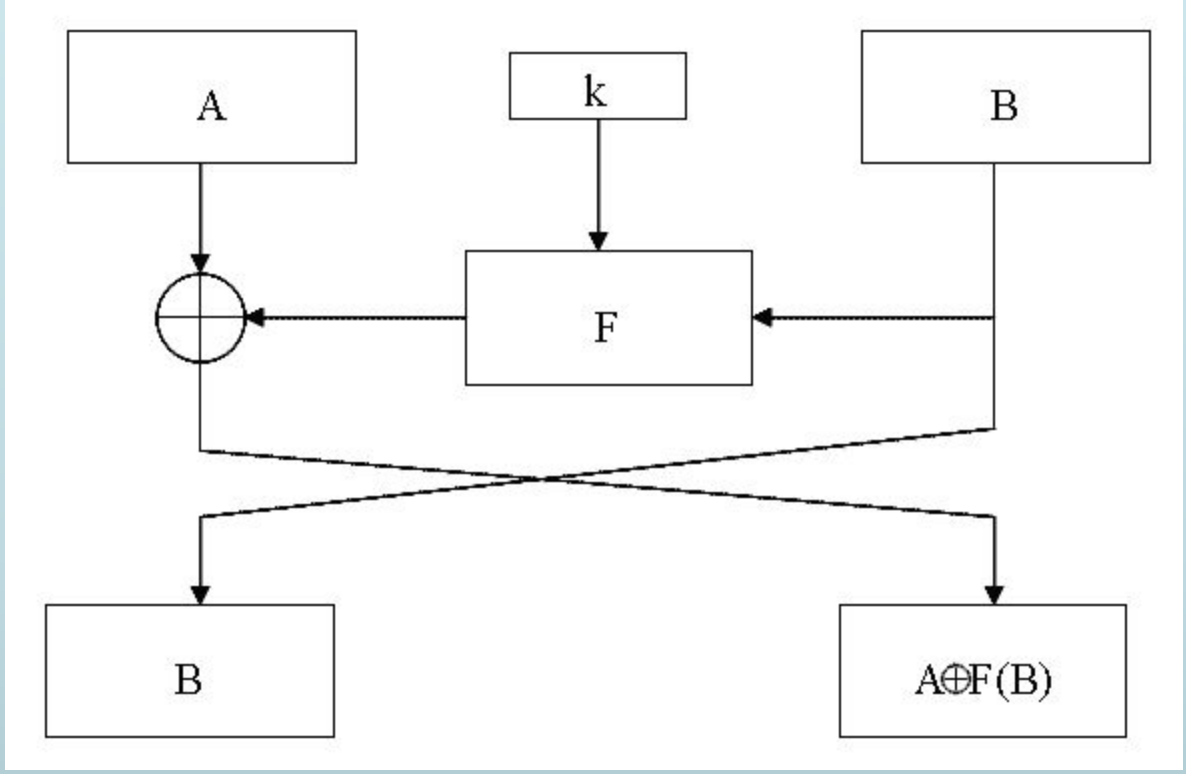
00110110 data XOR

01101100 res

- Определить какие два аргумента дали результат невозможно, хотя ф-я известна

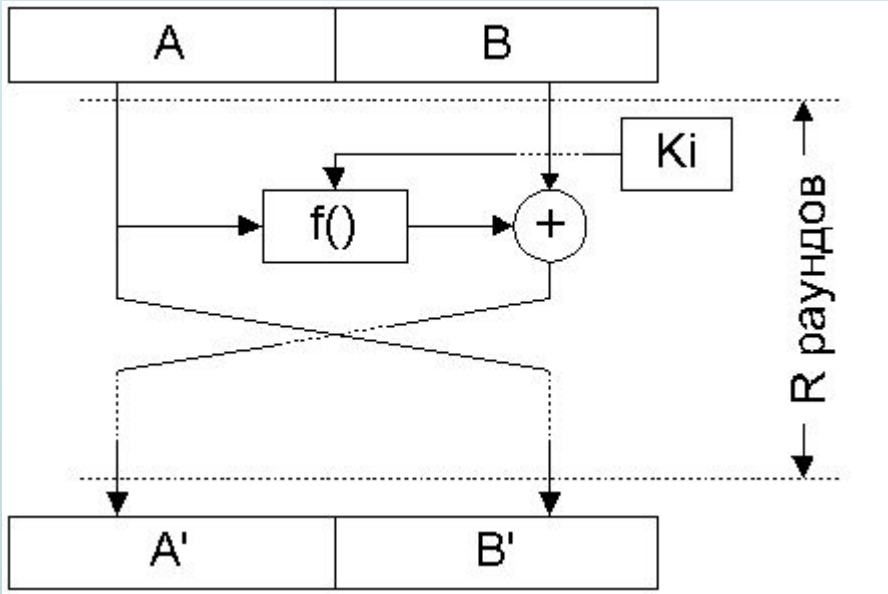
Сети Фейстеля

Упрощённый пример



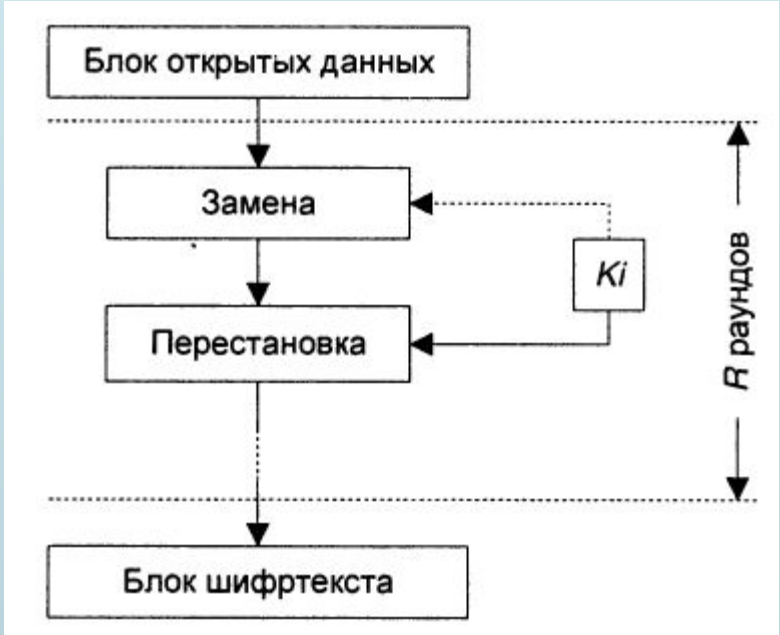
Сети Фейстеля

Большинство используемых сейчас алгоритмов шифрования эксплуатируют эту достаточно простую идею. В практическом плане варьируется количество раундов шифрования, сами функции F(вплоть до XOR), длины блоков. Иногда для усиления процедуры используются дополнительные шаги связанные с заменой содержания блоков, получившихся в каждом из раундов по заранее заготовленной таблицы.

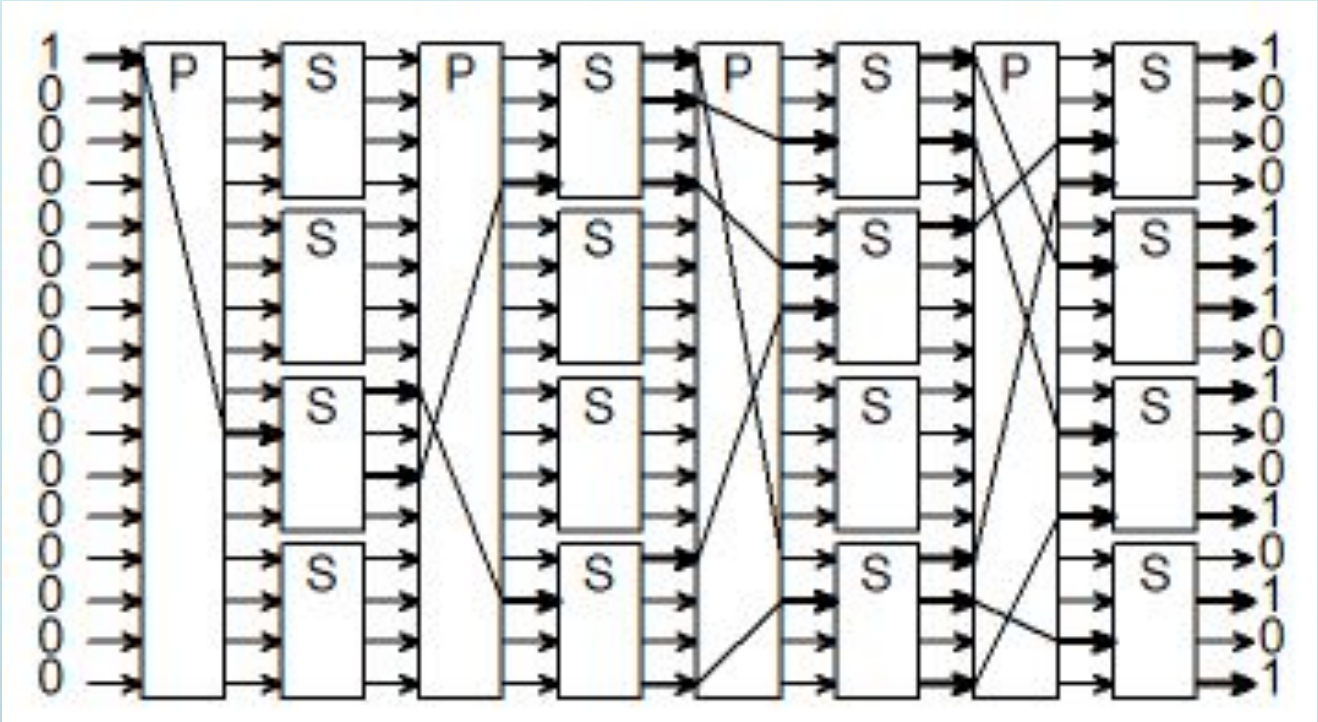


Подстановочно-перестановочные сети

- SP-сети
- В зависимости от ключа происходит замена целого блока открытого текста, по заранее заготовленной таблице, а затем перестановка заменённых фрагментов



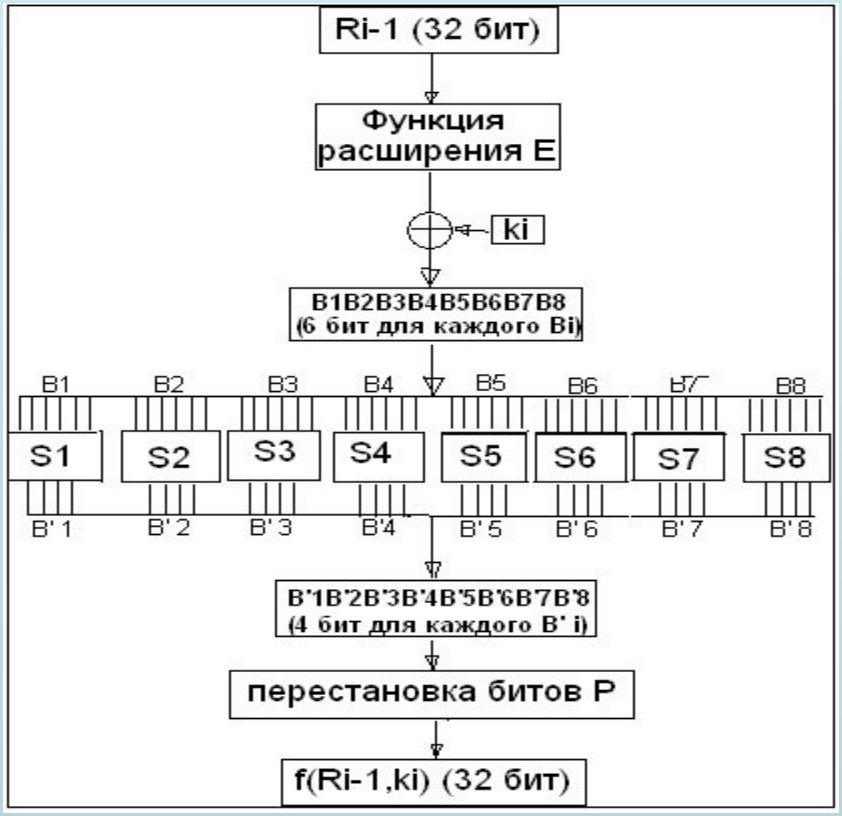
Подстановочно-перестановочные сети



Подстановочно-перестановочные сети

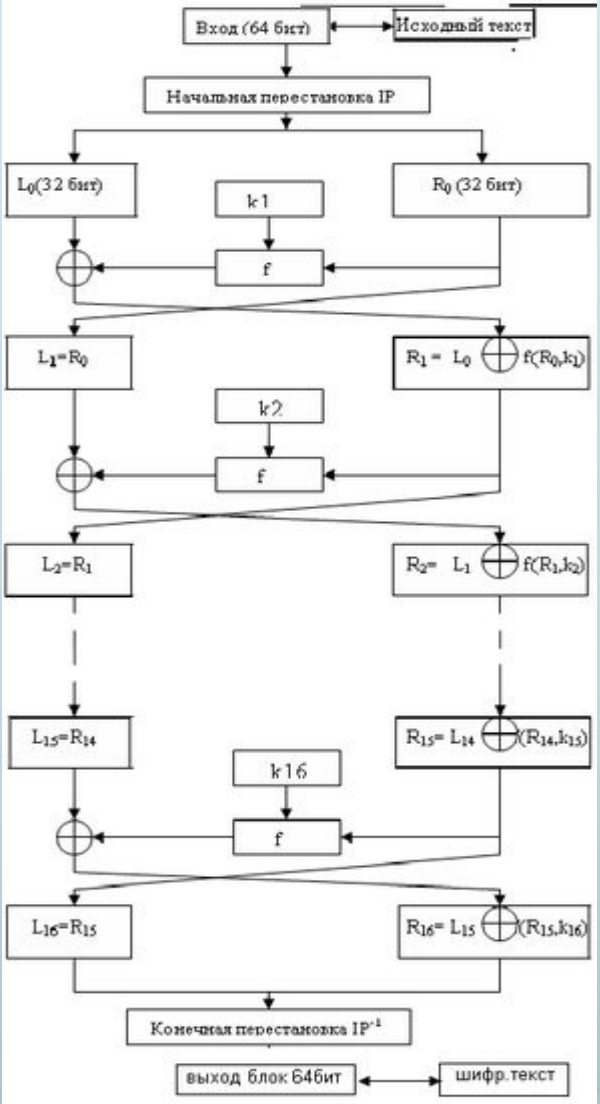
Фрагмент таблицы замены DES

	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	S_1
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	S_2
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	S_3
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	



B_3 = 101111, и мы хотим найти B'_3. Первый и последний разряды B_3 являются двоичной записью числа a, средние 4 разряда представляют число b. Строки таблицы S3 нумеруются от 0 до 3, столбцы таблицы S3 нумеруются от 0 до 15. Пара чисел (a, b) определяет число, находящееся в пересечении строки a и столбца b. Двоичное представление этого числа дает B'_3 . В нашем случае $a = 11_2 = 3$, $b = 0111_2 = 7$, а число, определяемое парой (3,7), равно 7. Его двоичное представление B'_3=0111.

Непротиворечивость



Алгоритм DES(который сейчас не считается достаточно безопасным) структурно является сетью Фейстеля, но его раундовая ф-я определяется таблицами расширения, замен и перестановок.

Расширение ключа

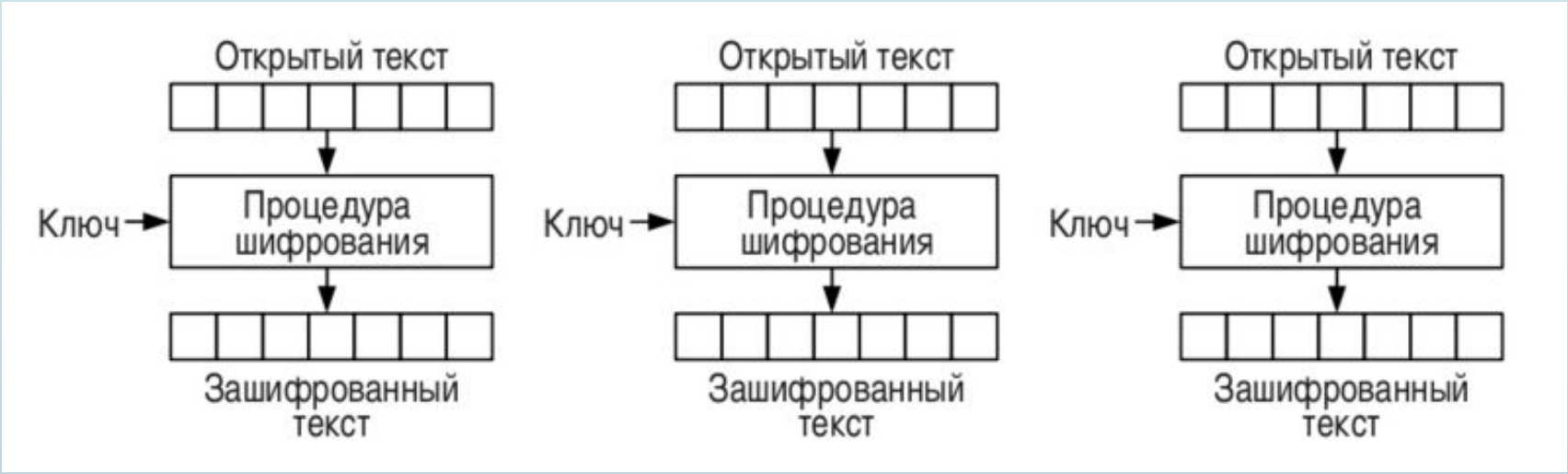
Процедура которая позволяет получить из общего ключа шифрования все раундовые ключи.
Может как примитивно разбивать исходный ключ на несколько ключей меньшего размера, определяя порядок их применения, так и определяться достаточно сложной математической процедурой.
Расширение ключа усиливает лавинный эффект и осложняет криптоанализ.

Режимы шифрования

- Electronic Codebook (ECB) – Электронная кодовая книга
- Cipher Block Chaining (CBC) – Сцепление блоков шифра
- Cipher Feedback (CFB) – Обратная связь по шифртексту
- Output Feedback (OFB) – Обратная связь по выходу
- Counter Mode (CTR)

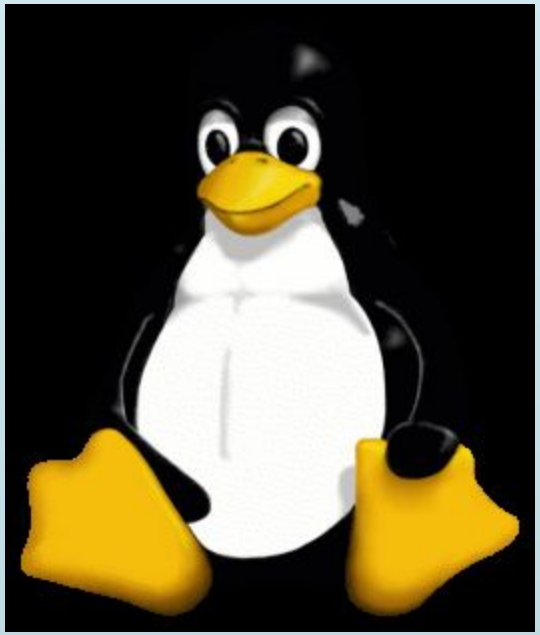
Electronic Codebook (ECB) – Электронная кодовая книга

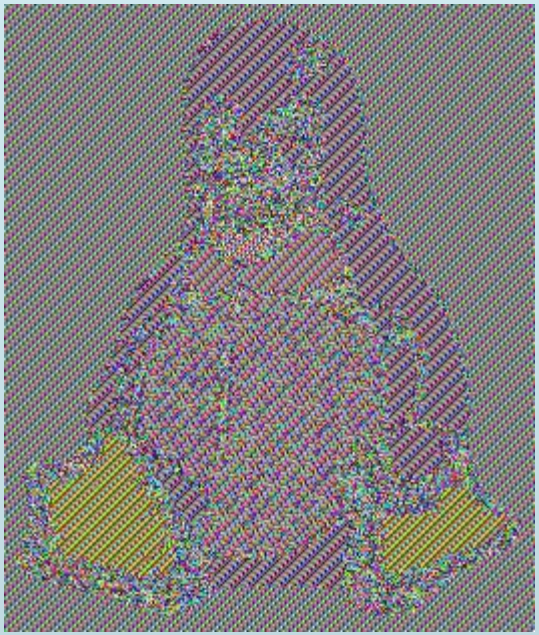
- Каждый блок открытого текста заменяется блоком шифротекста

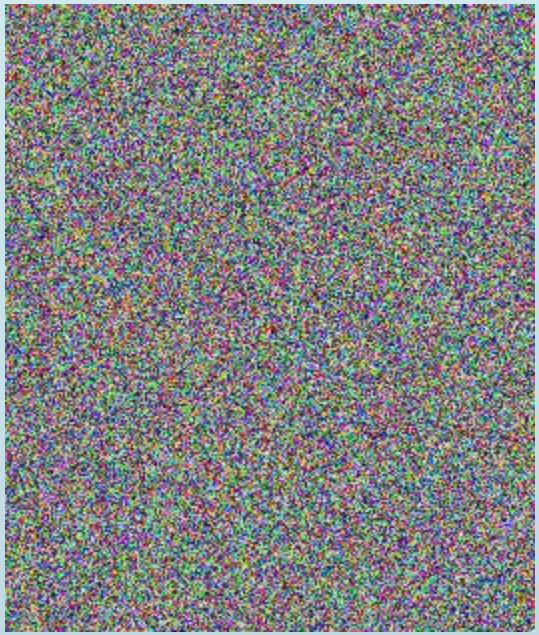


- Самый «слабый» из возможных режимов

Electronic Codebook (ECB) – Электронная кодовая книга

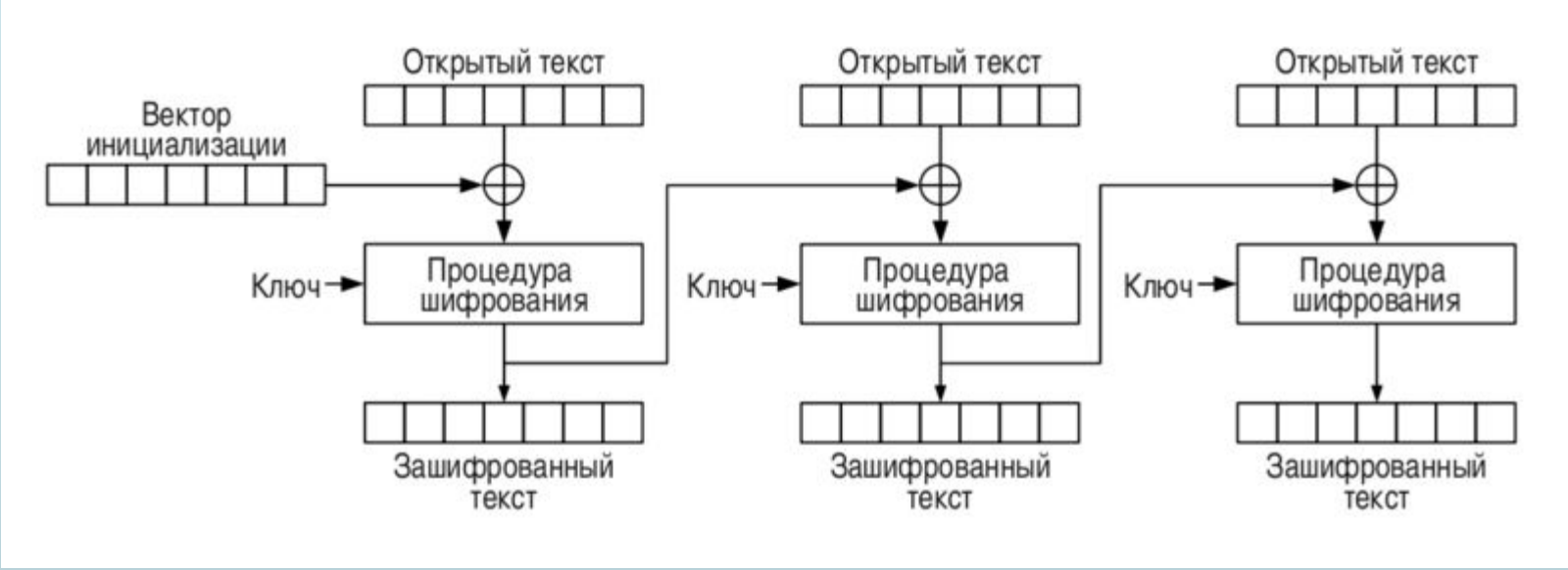






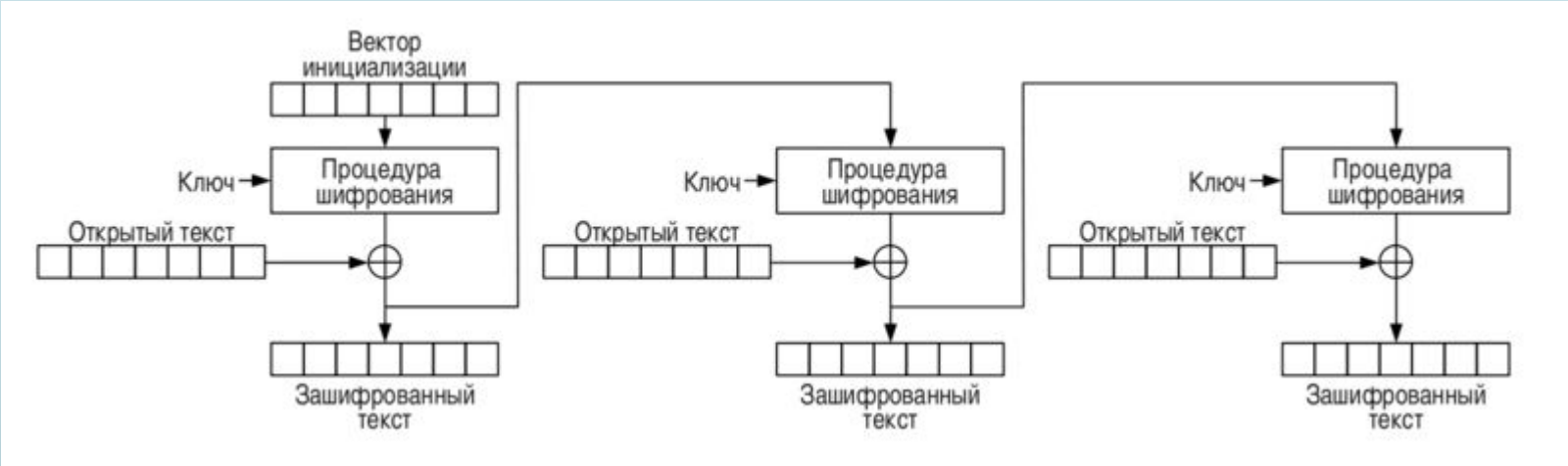
Cipher Block Chaining (CBC) – Сцепление блоков шифра

- Каждый блок открытого текста (кроме первого) побитово складывается по модулю 2 с предыдущим результатом шифрования.



Cipher Feedback (CFB)

- Для шифрования следующего блока открытого текста он складывается по модулю 2 с перешифрованным (блочным шифром) результатом шифрования предыдущего блока.



Атаки на симметричные шифры

- Нахождение текста сообщения
- Нахождение используемого ключа(полное раскрытие алгоритма шифрования)

- Нахождение эквивалентного ключа
- Нахождение части ключа

Атаки на симметричные шифры

- Атаки с известным шифртекстом
- При наличии шифратора в своём распоряжении могут быть применены следующие атаки
  - Атака с известным открытым текстом
  - Атака с выбранным открытым текстом
  - Атака с выбором шифртекста

Криптостойкость

- Криптостойкость определяется количеством следующих ресурсов требуемых для атаки
  - Количество информации необходимое для осуществления атаки
  - Время необходимое для осуществления атаки
  - Память необходимая для осуществления атаки

  или

  Не существует методов вскрытия отличных от метода «грубой силы», при этом длинна используемого ключа не позволяет эффективно применить такой метод

Запас криптостойкости

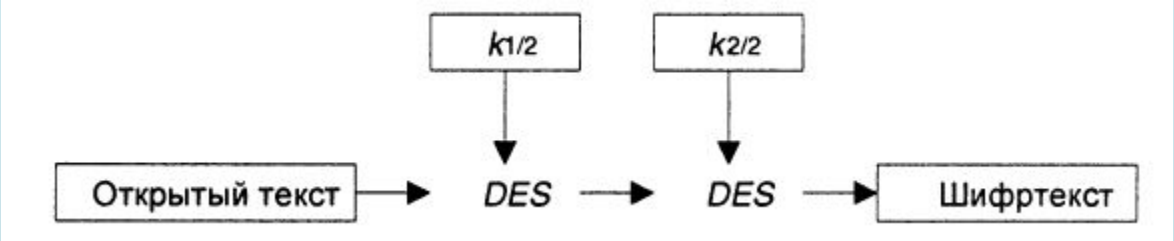
- Понятие используется при сравнении алгоритмов шифрования
- Даёт представление о том насколько надо упростить известный алгоритм, для осуществления эффективных атак

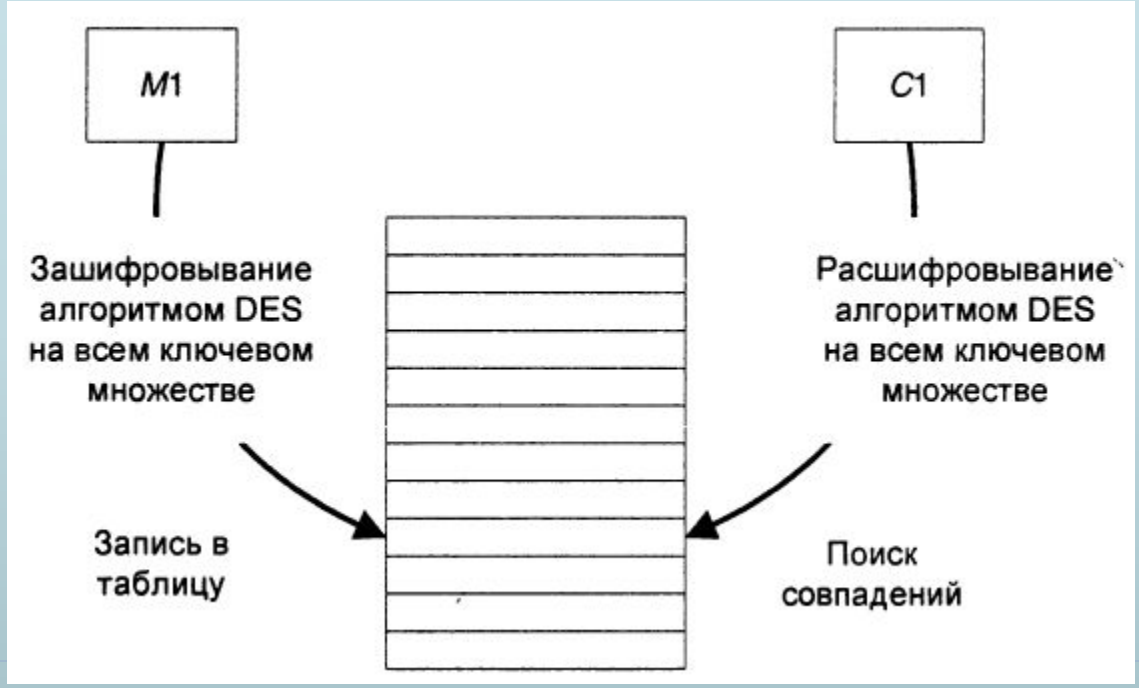
При удалении из структуры раунда SkipJack трёх из трёхсот двадцати предусмотренных операций XOR, ключ может быть вскрыт при наличии 2^9 выбранных открытых текстом и соответствующих им шифр текстов, с использованием порядка 10^6 тестовых операций

Метод грубой силы

- Перебор всех возможных ключей
- При неизвестном открытом тексте, считается, что размер шифр текста для осуществления данной атаки должен быть больше числа букв в алфавите (точка единственности)
- Использование информации о контрольной сумме сообщения

Встреча по середине(на примере Double DES-112 bit)





Дифференциальный криптоанализ

- Выбираются два открытых текста с известной разностью(например XOR)
- После зашифровывания оценивается разность шифртекстов, в зависимости от применённого алгоритма шифрования информация об изменении разности, может сузить пространство возможных ключей

Алгоритм RC5 вскрывается таким методом при наличии 2^44 пар выбранных текстов

Алгоритм GDES с 16 раундами и 256 битным ключом вскрывается при наличии 6 пар выбранных текстов

Линейный криптоанализ

- Эксплуатирует существование корреляции между некоторыми битами открытого текста, закрытого текста и ключа
- При наличии такой уязвимости можно делать догадки о некоторых битах используемых ключей

Остальные атаки

- Сдвиговая атака
- Метод бумеранга
- Метод интерполяции
- Невозможные дифференциалы
- Атаки с использованием утечки данных по побочным каналам

Знать

- Что такое симметричный шифр
- Чем блочное шифрование отличается от поточного
- Что такое рассеивание и полнота
- Какие существуют режимы шифрования
- Что такое сеть Фейстеля и SP-блоки
- Что такое вычислительно необратимые ф-и
- Какие существуют атаки на алгоритмы шифрования(как в смысле классификации, так и в смысле конкретных атак)
- Что такое запас криптостойкости
- Что такое раунд