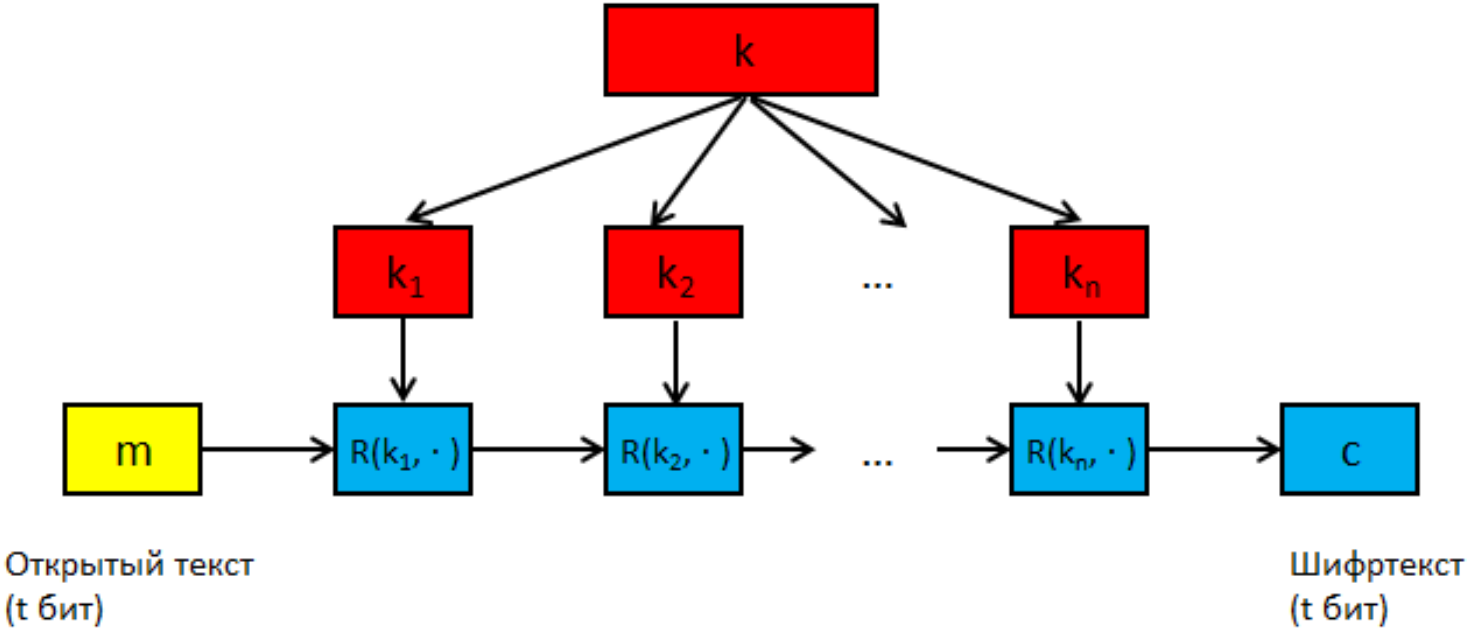
Информационная безопасность

Современные симметричные шифры

(презентация к лекции 2)

Амелин Р. В. Информационная безопасность. Конспект лекций // Амелин Р.В. Лаборатория преподавателя [Электронный ресурс]. URL: rv-lab.ru (2017).

Блочный шифр



k – секретный ключ

k_1 ... k_n – ключи раунда

n – число раундов

R – функция раунда

m – блок открытого текста

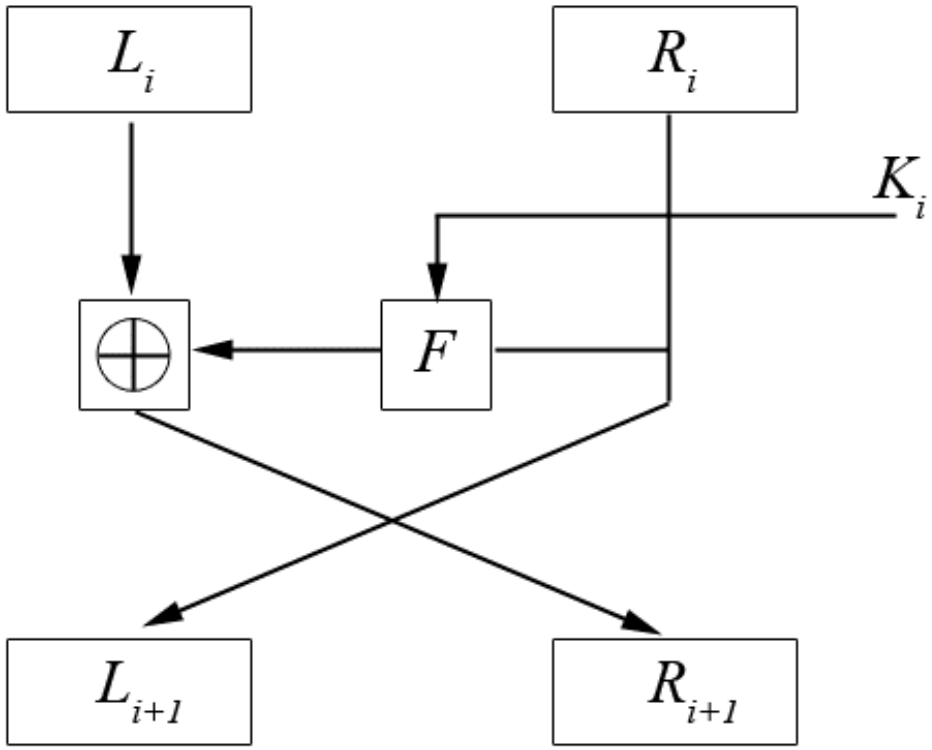
c – блок шифртекста

Конкретные шифры отличаются:

1. Длиной ключа
2. Размером блока
3. Числом раундов обработки
4. Алгоритмом генерации ключей раунда
5. Функцией раунда

Схема Файстеля

i-й раунд



Функция раунда *F* может быть необратимой (т.е. не существует F^{-1})

При этом независимо от выбранной функции *F* дешифрование будет выполняться по той же схеме (только ключи раунда применяются в обратном порядке)

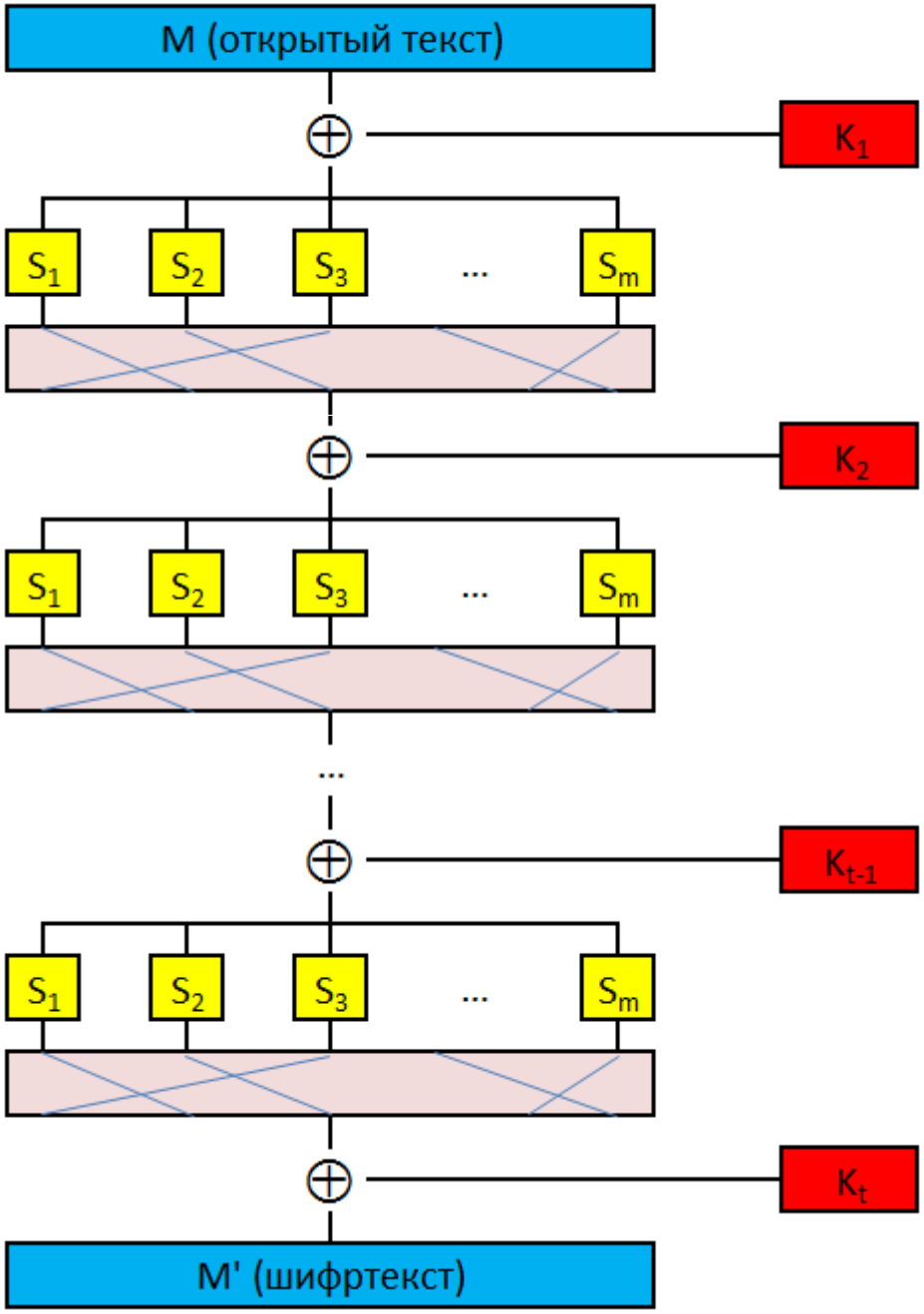
Конкретные шифры отличаются:

1. Длиной ключа
2. Размером блока
3. Числом раундов обработки
4. Алгоритмом генерации ключей раунда
5. Функциями раунда

Сеть подстановок и перестановок

Все подстановки и перестановки должны быть **обратимыми**

Пример: **алгоритм AES**
Длина блока 128 бит
Длина ключа раунда: 128 бит
Число раундов: 11
S-подстановка размером 8 бит
(16 внутренних блоков)



Вычислительная сложность

Вычислительная сложность алгоритма T(n) – это зависимость объема работы от размера входных данных.

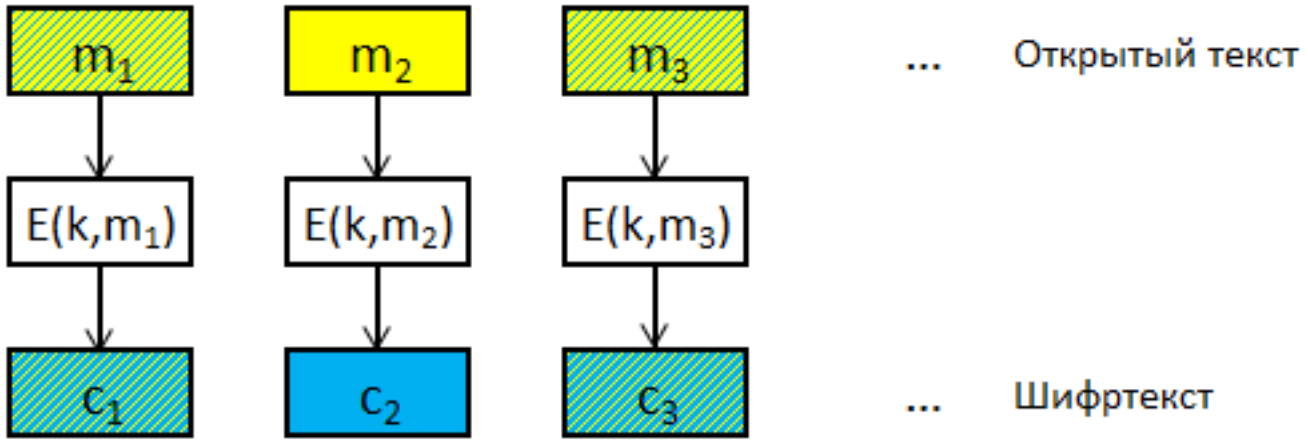
Нахождение точной зависимости зачастую нетривиально; используется *асимптотическая оценка*. Функция T(n) имеет порядок O(f(n)), если $\exists$ k, n_0 т. что $\forall$ $n > n_0$ $T(n) \le k*f(n)$. Т.е. T(n) растет не быстрее f(n).

Виды сложности (по возрастанию):

Константная	K	Обращение к элементу массива по индексу
Логарифмическая	K * log(n)	Бинарный поиск
Линейная	K * n	Перебор элементов массива
Линейный логарифм	n * log(n)	Алгоритмы быстрой сортировки
Полиномиальная	n^K	Алгоритмы простой сортировки (*пузырьком*)
Экспоненциальная	K^n	Алгоритмы перебора (*brute force*)
Факториальная	n!	Алгоритмы комбинаторики (сочетания, перестановки и т.д.)

Режимы блочных шифров

Режим электронной кодовой книги (ECB)



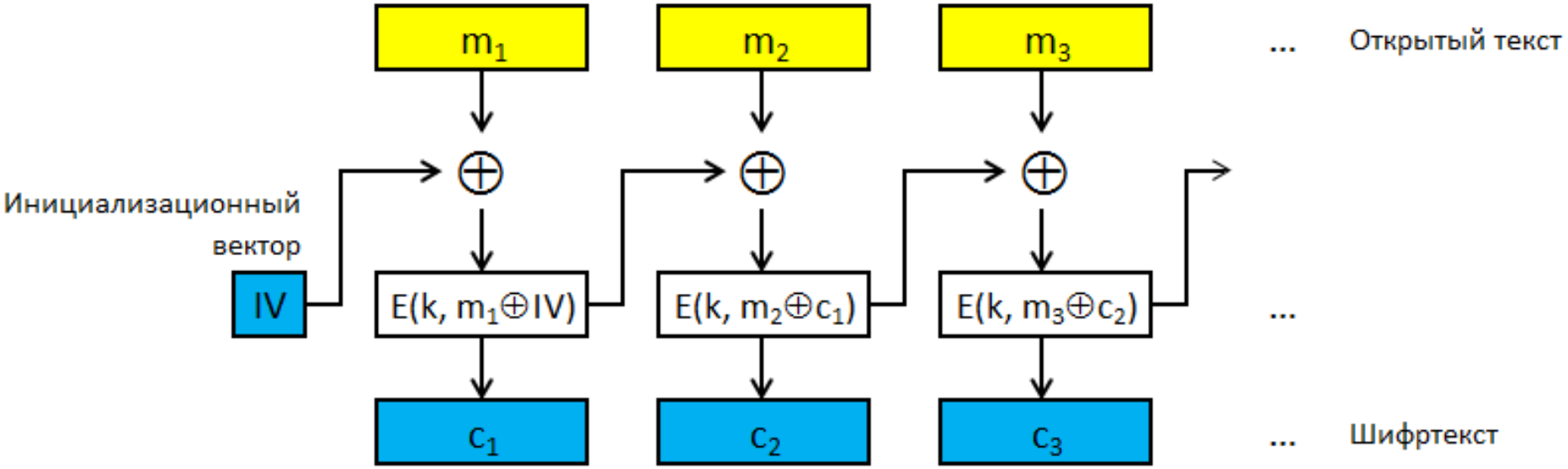
Одинаковые блоки открытого текста переходят в одинаковые блоки зашифрованного текста

Противник получает информацию об открытом тексте (даже если он не сможет расшифровать эти блоки). Например, наблюдая за зашифрованным файлом на диске, он видит, какие его участки меняются в процессе редактирования

Режим ECB **является небезопасным** и **не должен использоваться**

Режимы блочных шифров

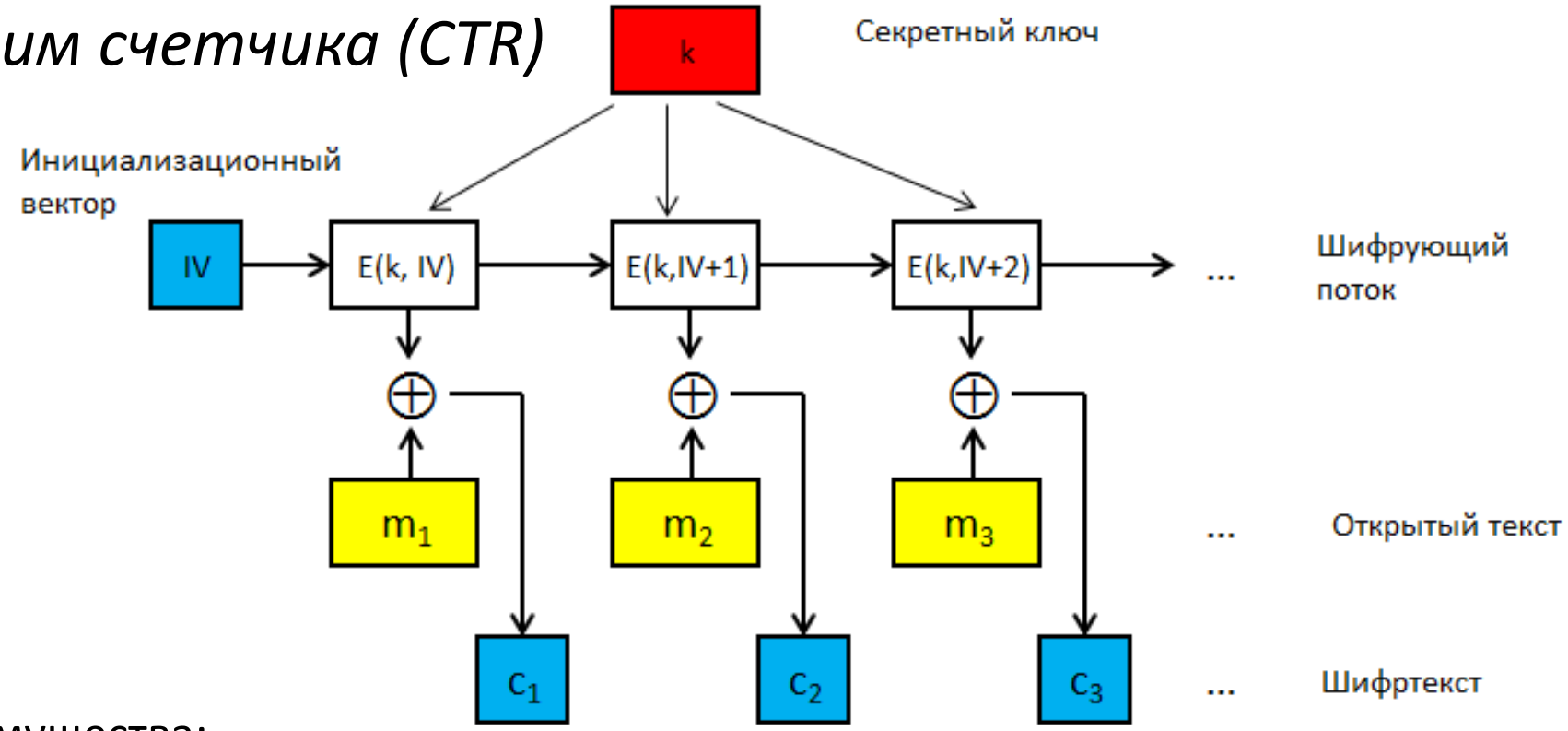
Режим сцепления шифрованных блоков (CBC)



- Перед шифрованием сообщение *дополняется* до длины, кратной длине блока. Варианты дополнения:
  - $1000\ldots0$
  - $l \,||\, l \,||\, l \,||\, l \ldots$, где l – длина сообщения
- Инициализационный вектор пересылается вместе с шифртекстом

Режимы блочных шифров

Режим счетчика (CTR)

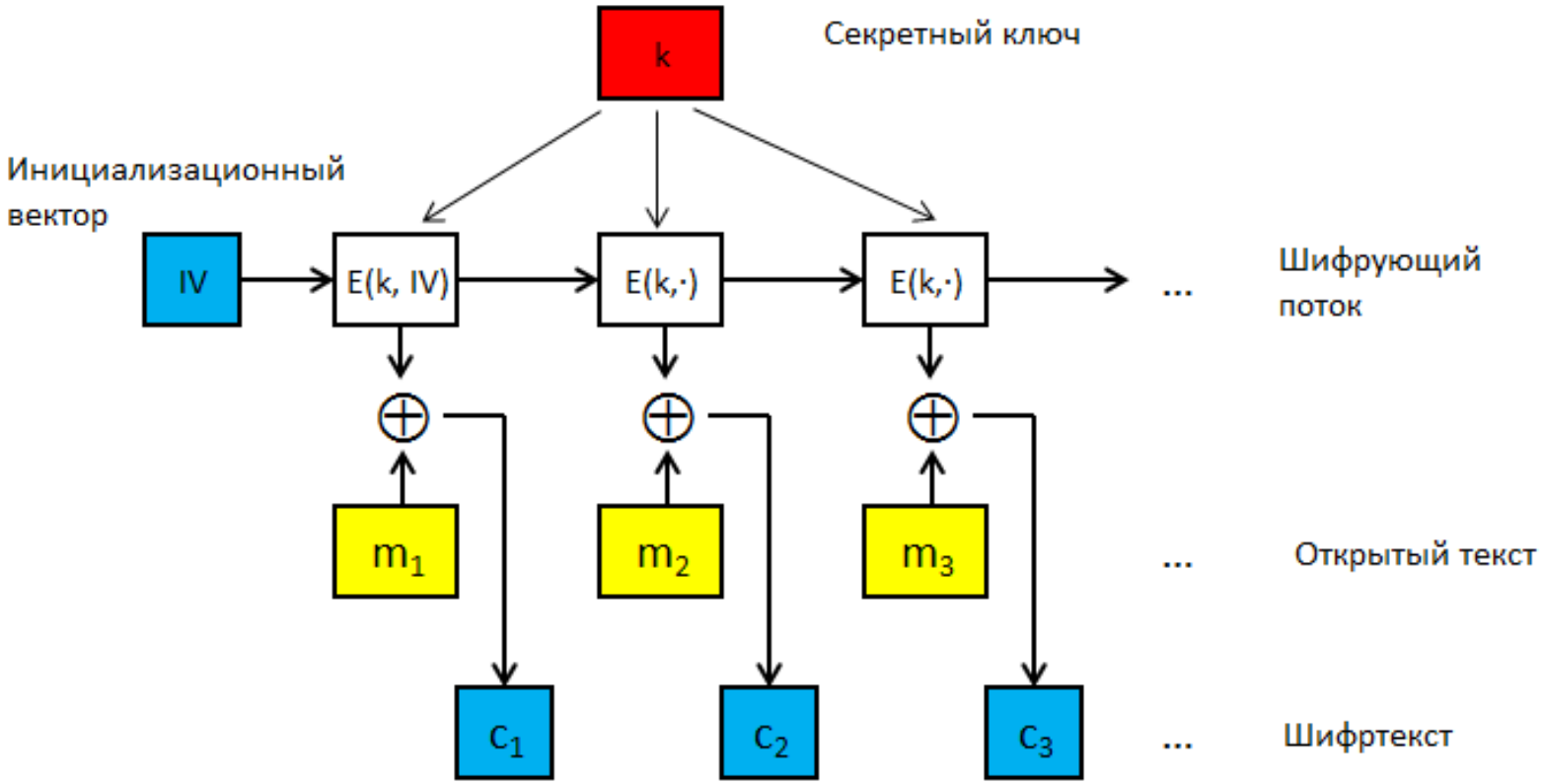


Преимущества:

- Возможность распараллеливания
- Нет необходимости набивки
- В качестве E может использоваться односторонняя функция
- Параметры безопасности лучше, чем у CBC

Режимы блочных шифров

Режим обратной связи по выходу (OFB)



В режимах OFB и CTR блочный шифр превращается в потоковый, т.е. генерируется шифрующая последовательность, которая складывается с открытым текстом операцией xor