ШИФРЫ ПОТОКА И БЛОЧНЫЕ ШИФРЫ

Студент: Шутенко Виктория Михайловна
Группа: НФИмд-02-23

Виды шифрования:

- поточные (потоковые) шифры;
- блочные шифры;
- блочные шифры с обратной связью.

Признаки шифрования

Тип криптосистемы	Операции с битами или блоками	Зависимость от предыдущих знаков	Позиционная зависимость	Наличие симметрии функции шифрования
Поточного шифрования	Биты	Не зависит	Зависит	Симметричная
Блочного шифрования	Блоки	Не зависит	Не зависит	Симметричная или несимметричная
С обратной связью от шифротекста	Биты или блоки	Зависит	Не зависит	Симметричная

Потоковые шифры

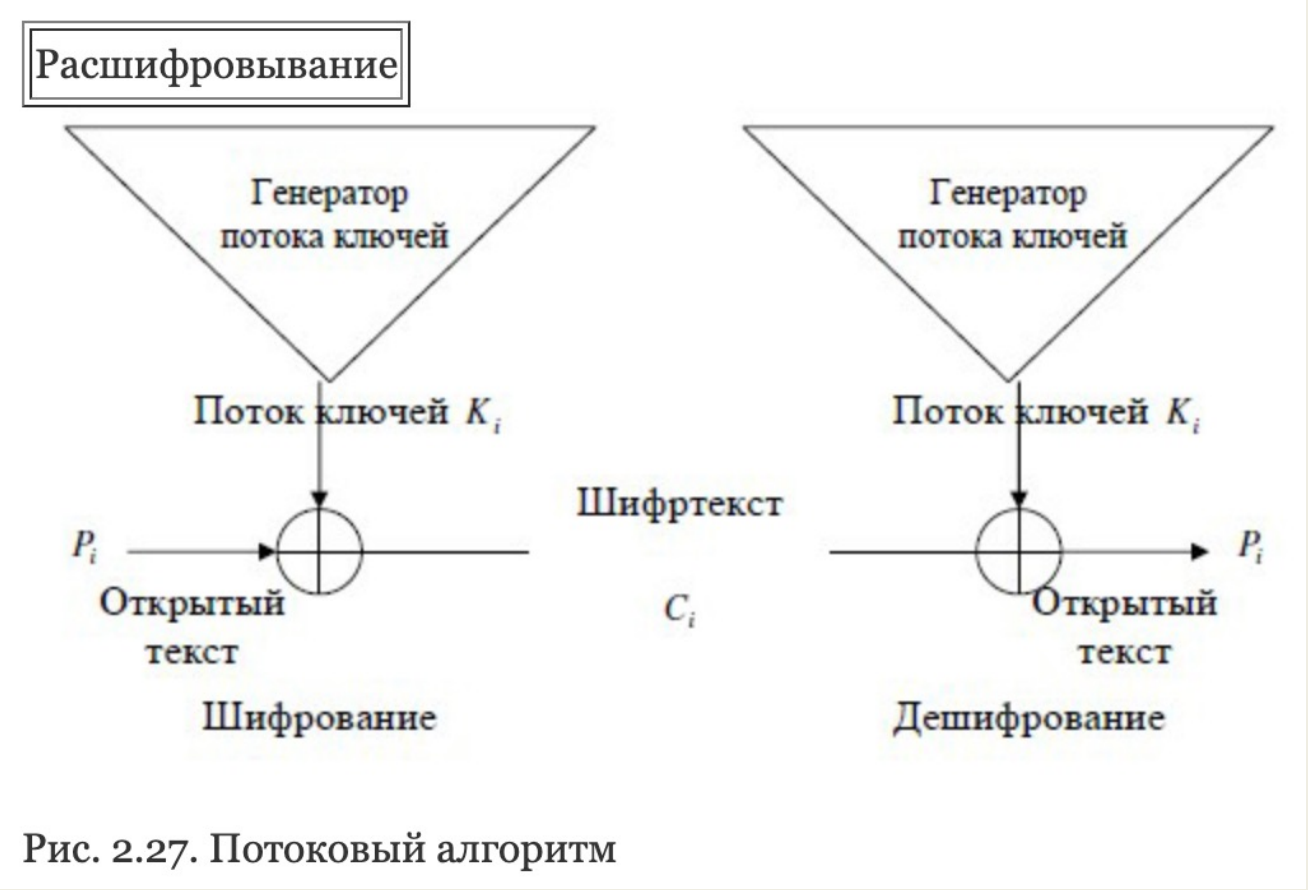
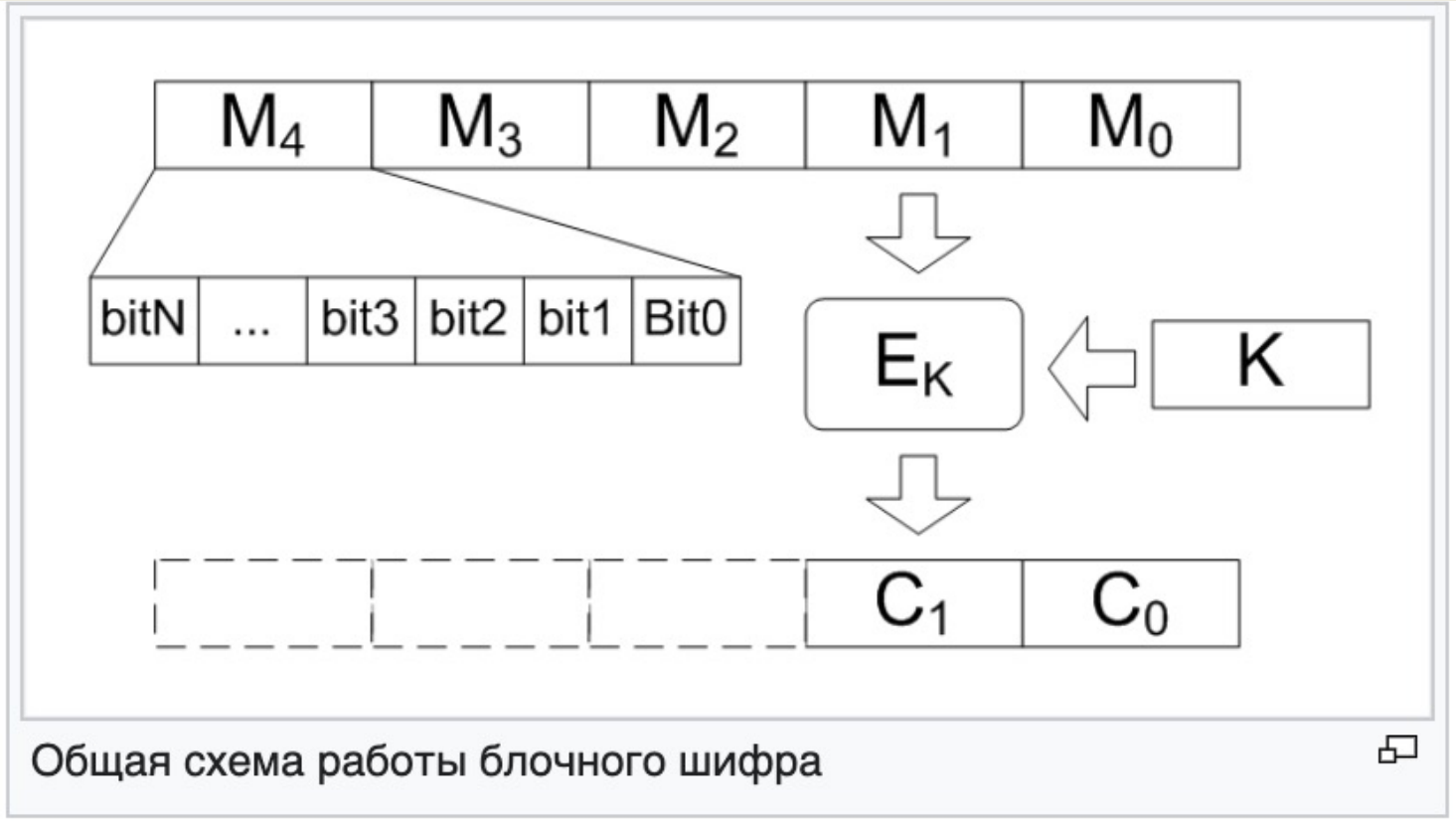


Рис. 2.27. Потоковый алгоритм

Достоинства и недостатки потоковых шифров

+	–
Высокая скорость при использовании	Необходимость информации синхронизации
Простота реализации	

Блочные шифры

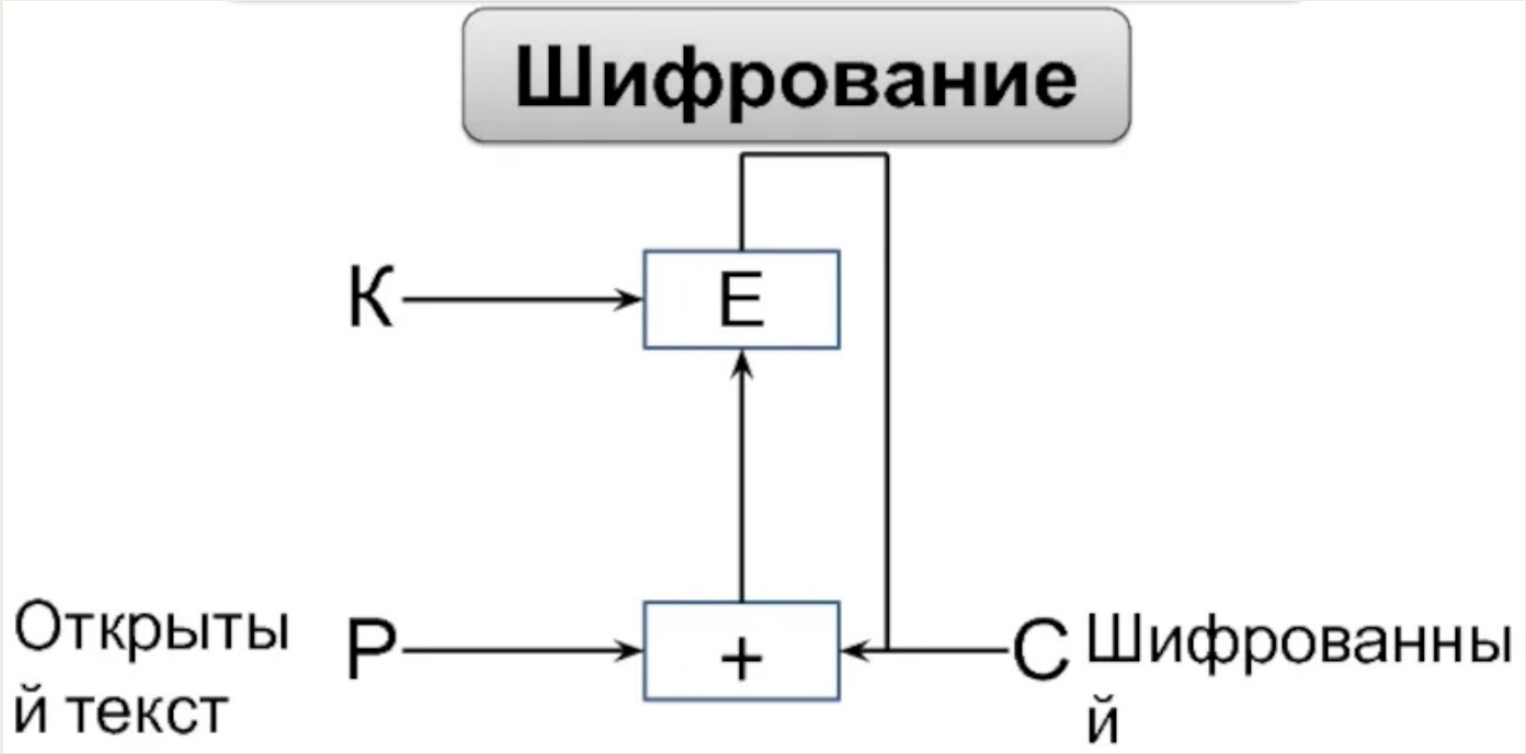


Общая схема работы блочного шифра

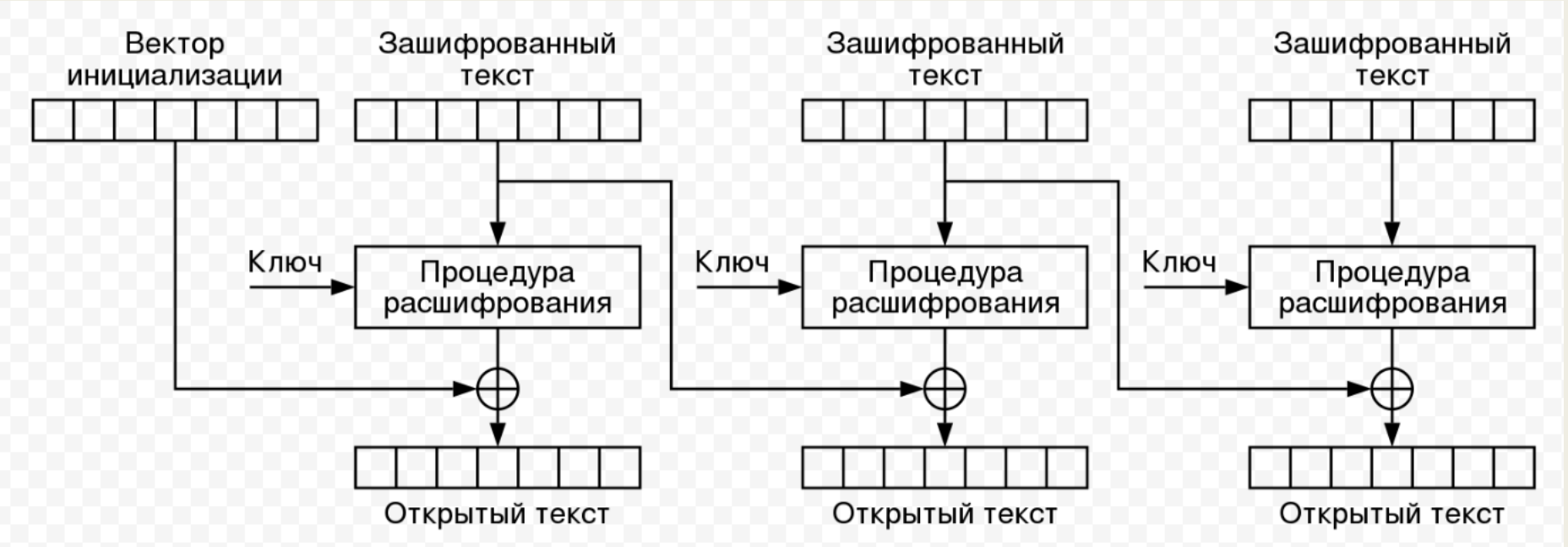
Режимы алгоритма DES блочного шифрования

- ECB (Electronic code Book);
- CBC (Cipher block chaining);
- CFB (Cipher feedback);
- OFB (Output feedback).

Блочное шифрование с обратной связью



Шифр со сцеплением блоков шифротекста CBC



Выводы

- Техника блочного шифрования включает в себя шифрование одного блока текста за раз.
- Блочный шифр использует режимы алгоритмов ECB (электронная кодовая книга) и CBC (цепочка блоков шифров) .
- Потоковый шифр использует функцию XOR для преобразования обычного текста в зашифрованный текст.
- Блочный шифр использует один и тот же ключ для шифрования каждого блока, в то время как потоковый шифр использует разные ключи для каждого байта.