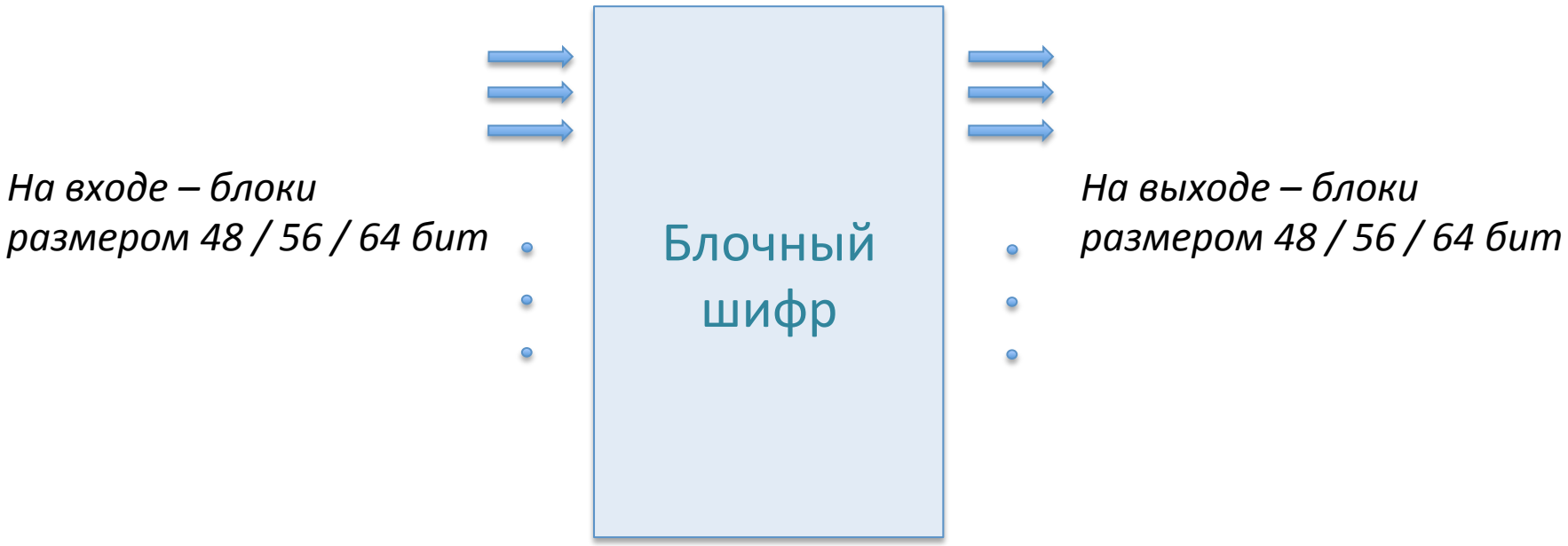
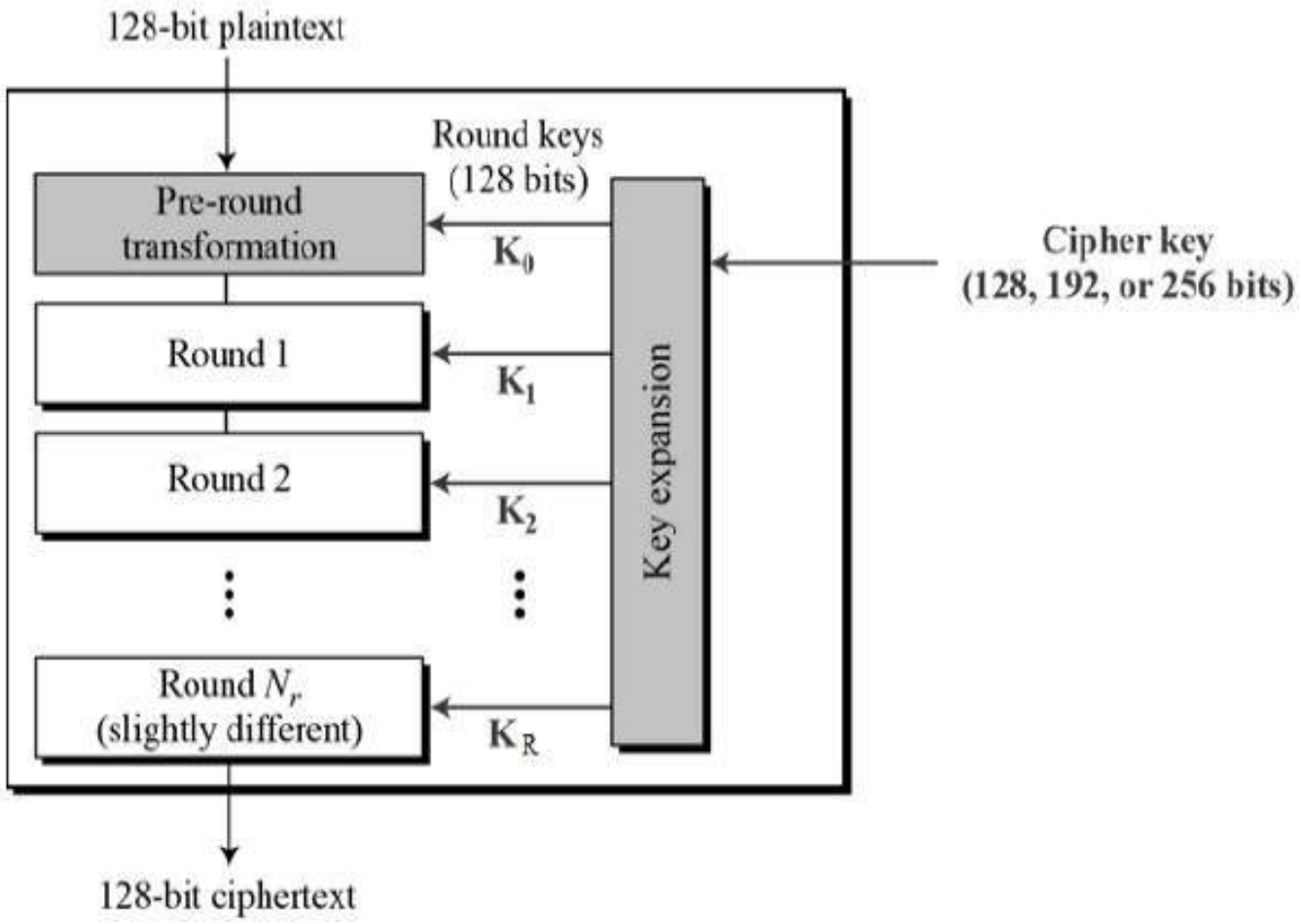
Симметричные блочные шифры



Осуществить качественное преобразование «за раз» крайне сложно. Поэтому блочные шифры построены по итеративному принципу.

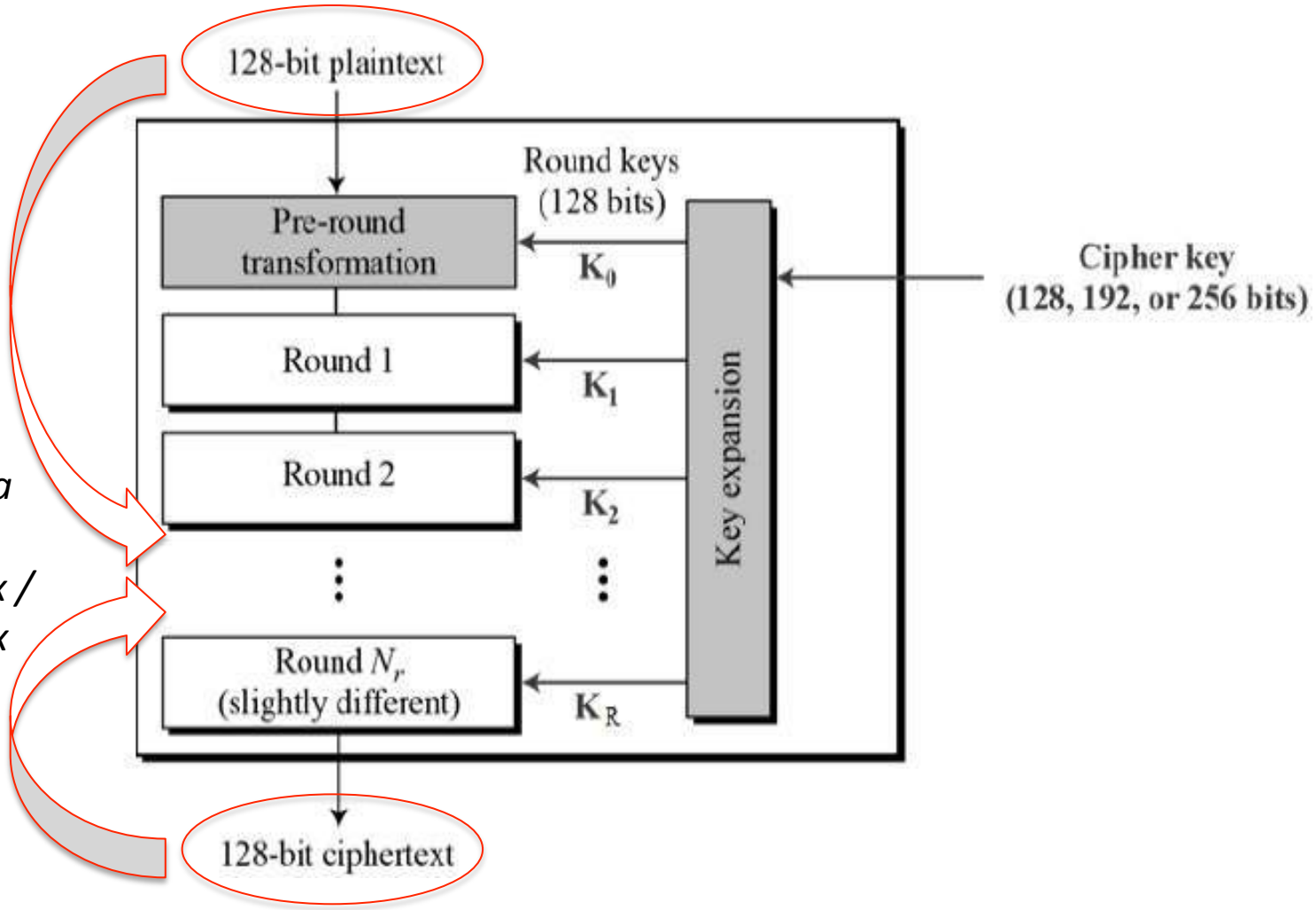
Итеративные блочные шифры



Трудности

- Как получить из основного ключа раундовые ключи (ключевое расписание)?
- Число раундов VS размер блока, качество раундовой функции
- «Инфолютивность» алгоритма шифрования (зашифрование = расшифрование)

Ключевое расписание



перебор упрощается, если не все биты ключа задействованы в нескольких первых / последних раундах