Компьютерная криптография

(с 70-х годов XX века)

Основные этапы развития криптографии

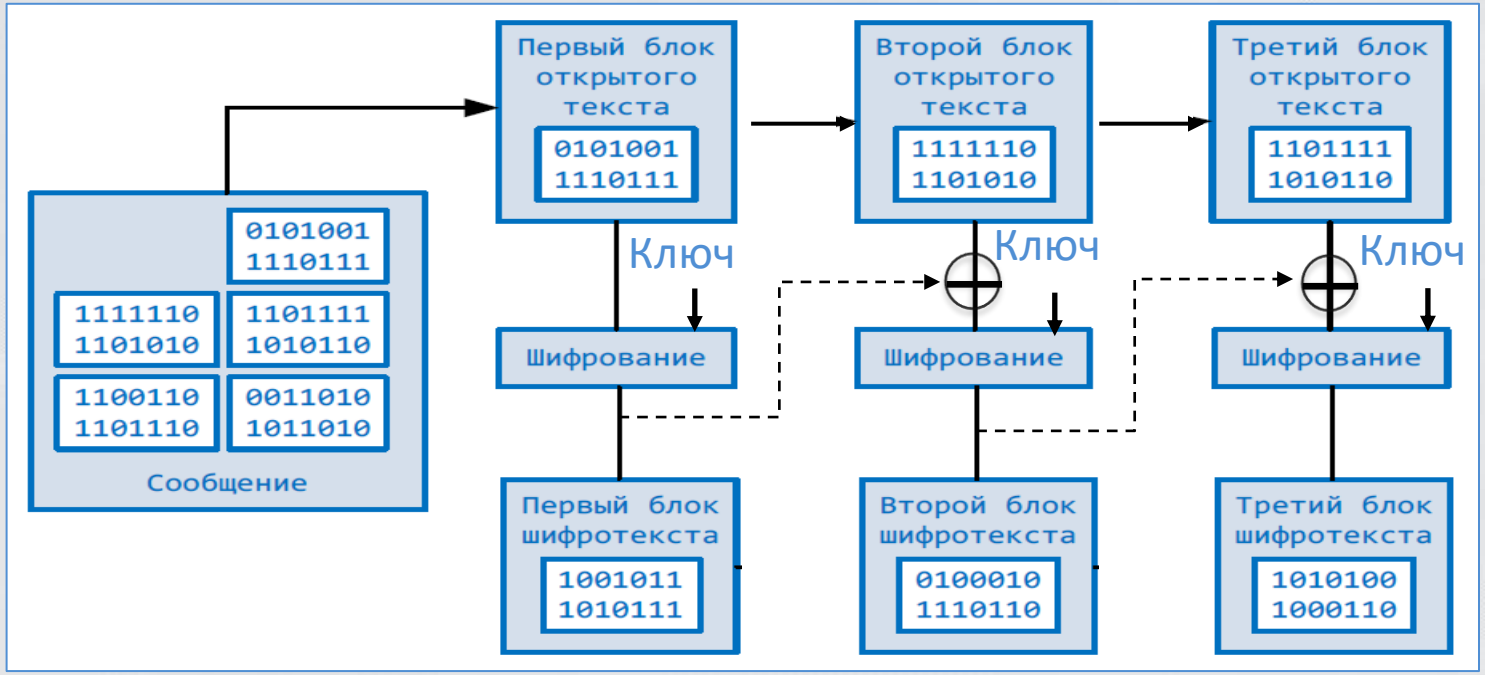
1. • Интуитивная (до начала XVI века)
2. • Формальная (конец XV века - начало XX века)
3. • Научная (30-е - 60-е годы XX века)
4. • Компьютерная (с 70-х годов XX века)

Модель протокола симметричного шифрования

Свойства модели

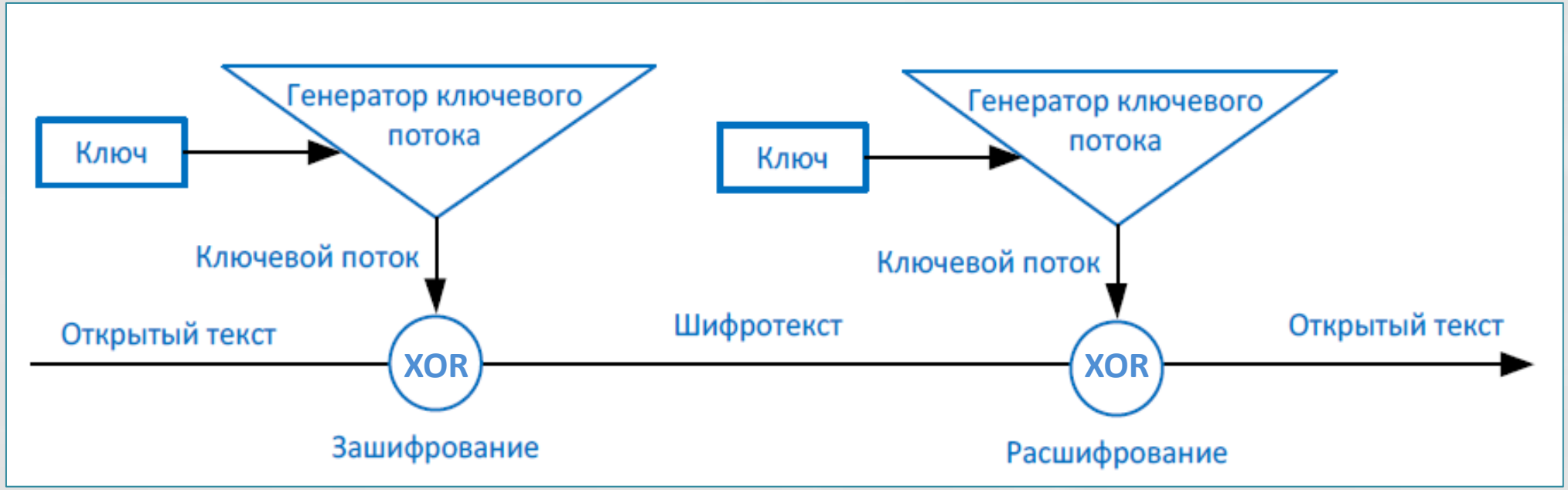
- Симметричные ключи (также называемые секретными ключами (*secret key*) - имеет двойную функциональность и применяется для зашифрования и для расшифрования
- Каждый из абонентов должен хранить ключ в секрете и надлежащим образом защищать его
- Поскольку оба абонента используют один и тот же ключ, то симметричные криптосистемы могут обеспечить только конфиденциальность, но не аутентификацию или неотказуемость

Блочный шифр



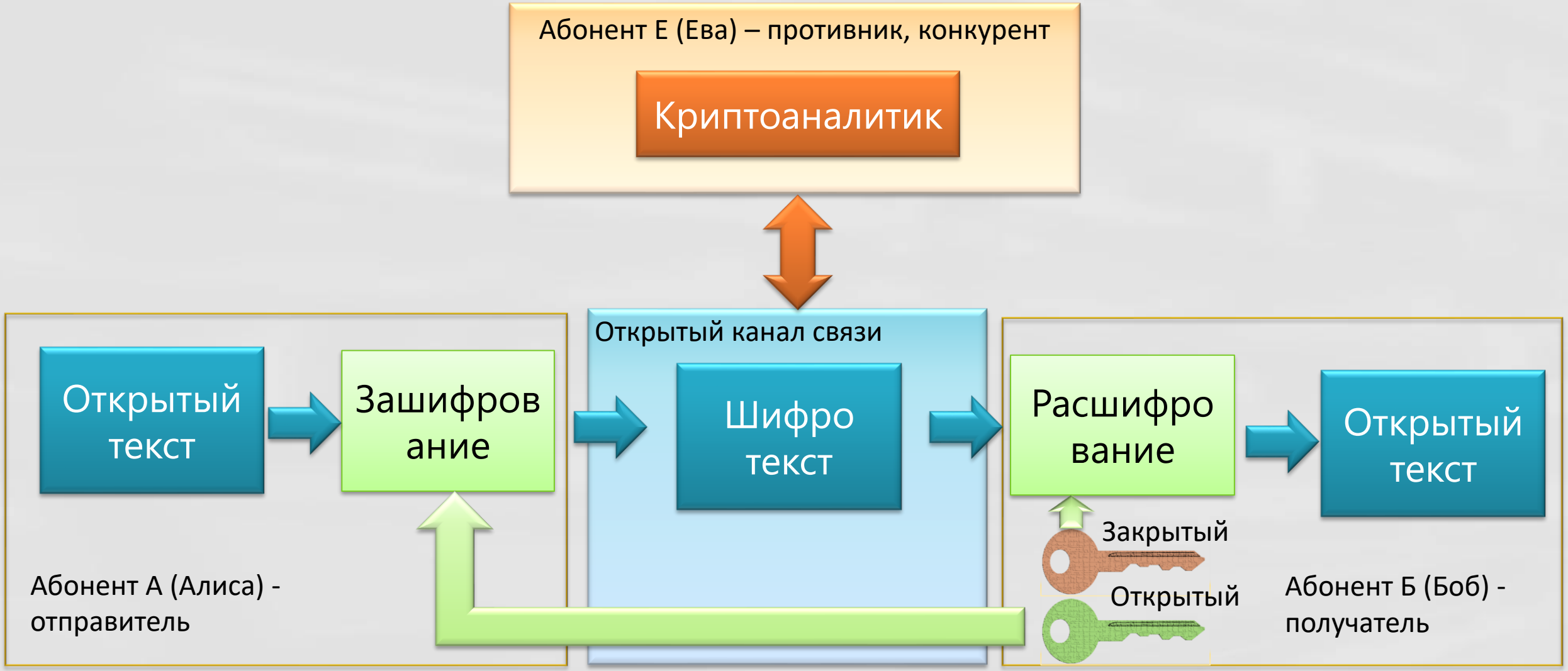
- Сообщение делится на блоки битов, которые передаются на обработку математическим функциям, по одному блоку за раз
- Для обеспечения стойкости шифра, в нем должны в достаточной степени использоваться два основных метода: перемешивание (confusion) и рассеивание (diffusion). Перемешивание обычно выполняется с помощью замены, тогда как рассеивание – с помощью перестановки.

Поточный шифр



- Поточные шифры (*stream cipher*) обрабатывают сообщение, как поток битов и выполняют математические функции над каждым битом отдельно
- Поточные шифры используют генератор ключевого потока, который производит поток битов, объединяемых с помощью операции XOR с битами открытого текста

Модель протокола асимметричного шифрования



Свойства модели

- В асимметричных системах для зашифровки и расшифровки используются различные (асимметричные) ключи, которые связаны между собой математически и образуют пару
- Открытый ключ (*public key*) может быть известен всем
- Закрытый ключ (*private key*) должен знать только его владелец
- Знание открытого ключа другого абонента не позволяет узнать соответствующий ему закрытый ключ

Использование асимметричных ключей

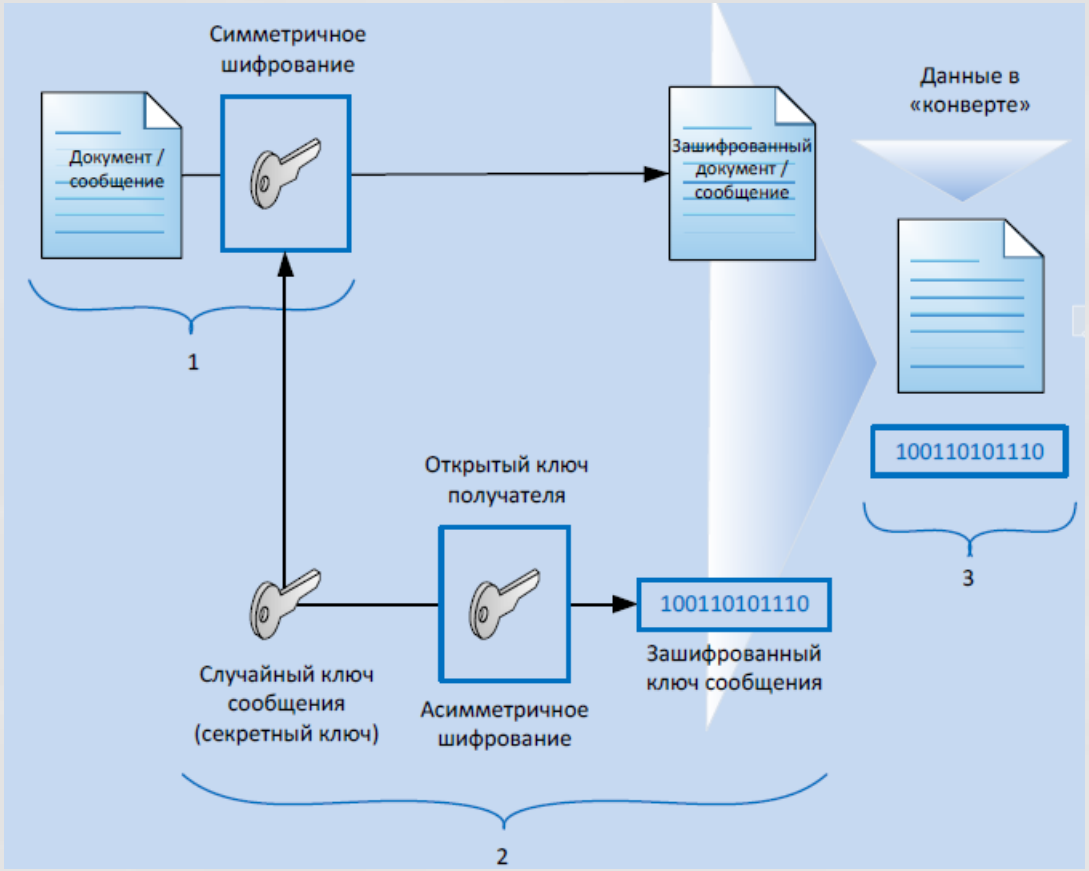
- Конфиденциальность обеспечивается зашифровкой сообщения на открытом ключе получателя. Такую зашифровку называют закрытым форматом сообщения (*secure message format*)
- Аутентификация обеспечивается зашифровкой на закрытом (приватном) ключе отправителя. Такую зашифровку называют открытым форматом сообщения (*open message format*)

Сравнение моделей шифрования

Атрибут	Симметричный	Асимметричный
Ключи	Один ключ используется совместно двумя или более субъектами	Один субъект имеет открытый ключ, другой субъект – соответствующий ему закрытый ключ
Обмен ключами	Нестандартный защищенный механизм	Открытый ключ делается общедоступным, а закрытый ключ хранит в секрете его владелец
Скорость	Алгоритм менее сложный и поэтому быстрый	Алгоритм более сложный и поэтому медленный
Использование	Комплексное шифрование (т.е. шифрование файлов и коммуникационных каналов)	Распространение ключей и цифровые подписи
Предоставляемые сервисы безопасности	Конфиденциальность	Аутентификация и неотказуемость

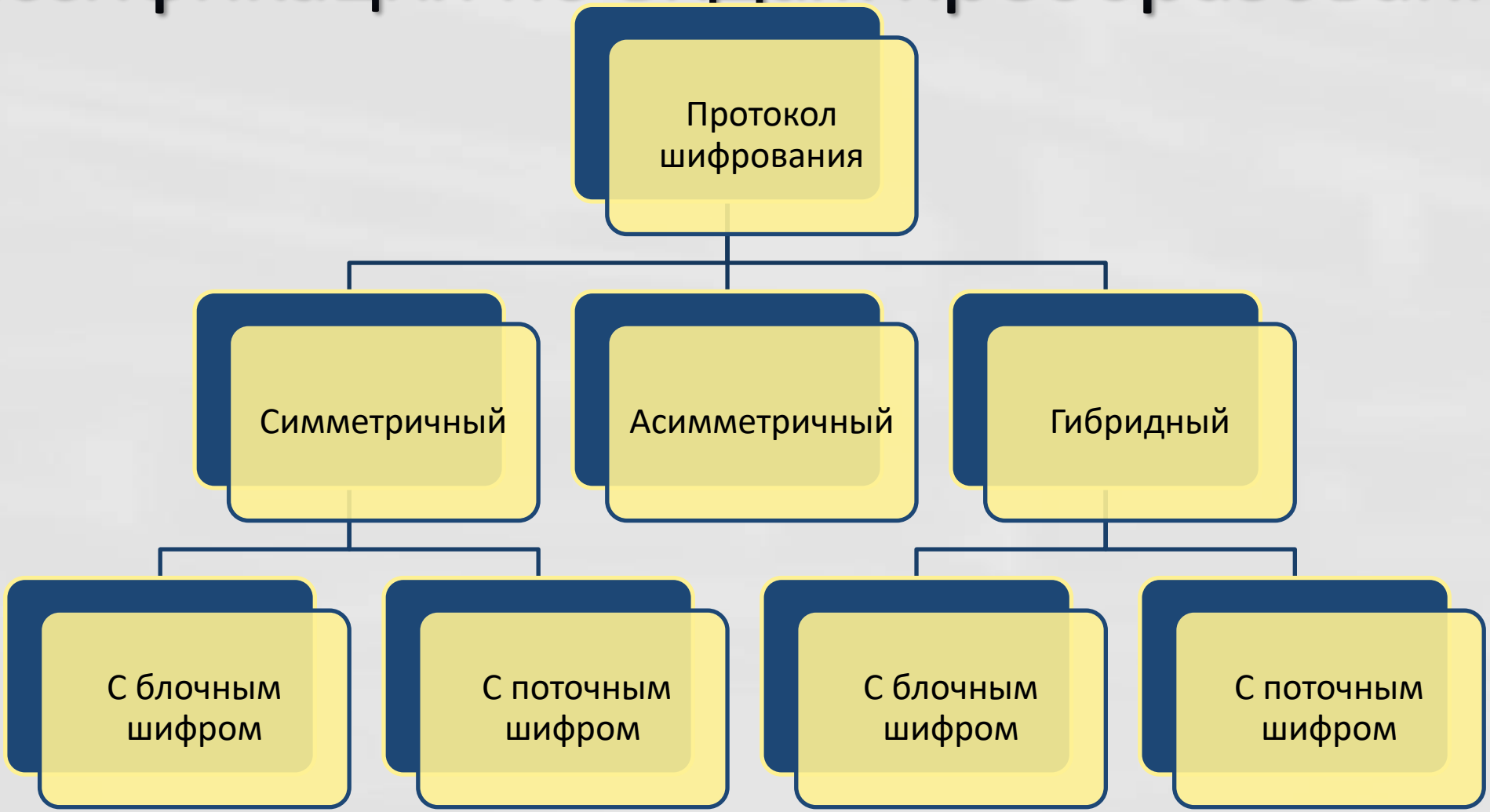
Модель протокола гибридного шифрования

Пример протокола гибридного шифрования



- 1. Сообщение шифруется симметричным секретным ключом
- 2. Секретный ключ шифруется открытым ключом получателя
- 3. Зашифрованное сообщение и зашифрованный ключ составляют цифровой конверт (*digital envelope*), который отправляется получателю
- 4. Получатель сначала расшифровывает секретный ключ, а затем расшифровывает секретным (сеансовым) ключом шифротекст сообщения

Классификация по видам преобразований



Классификация по видам криптостойкости