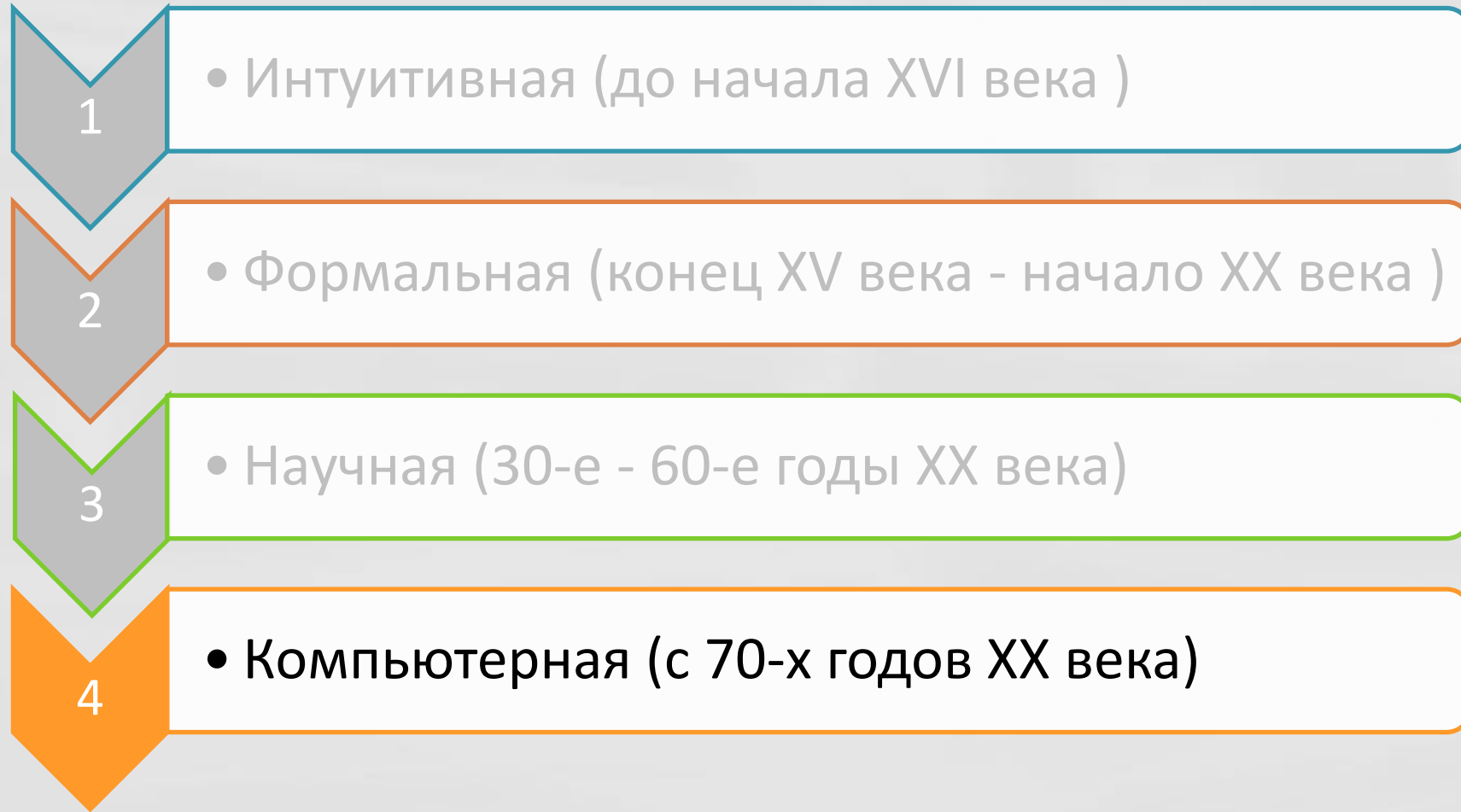


# *Компьютерная криптография*

*(с 70-х годов XX века)*

# Основные этапы развития криптографии



# Модель протокола симметричного шифрования

Абонент Е (Ева) – противник, конкурент

Криптоаналитик



Открытый канал связи

Открытый  
текст



Зашифров  
ание



Шифро  
текст



Расшифро  
вание



Открытый  
текст

Абонент А (Алиса) -  
отправитель

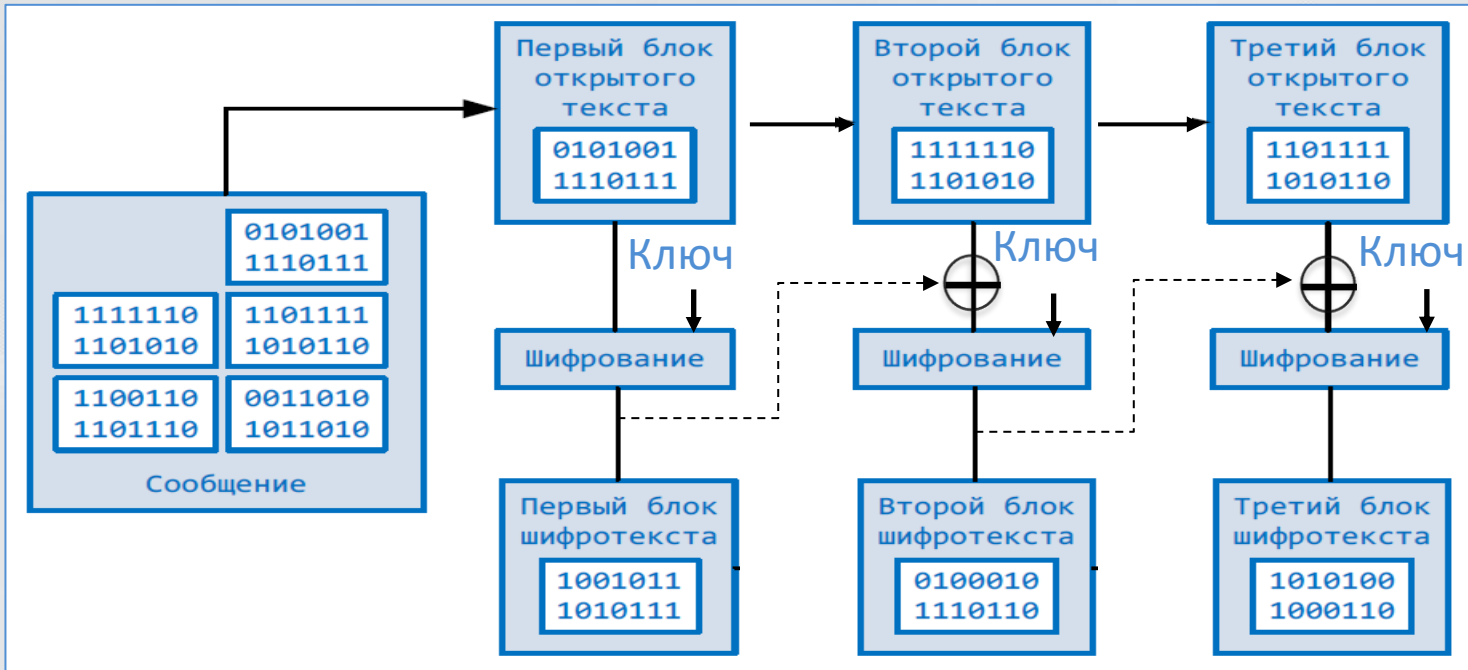


Абонент Б (Боб) -  
получатель

# Свойства модели

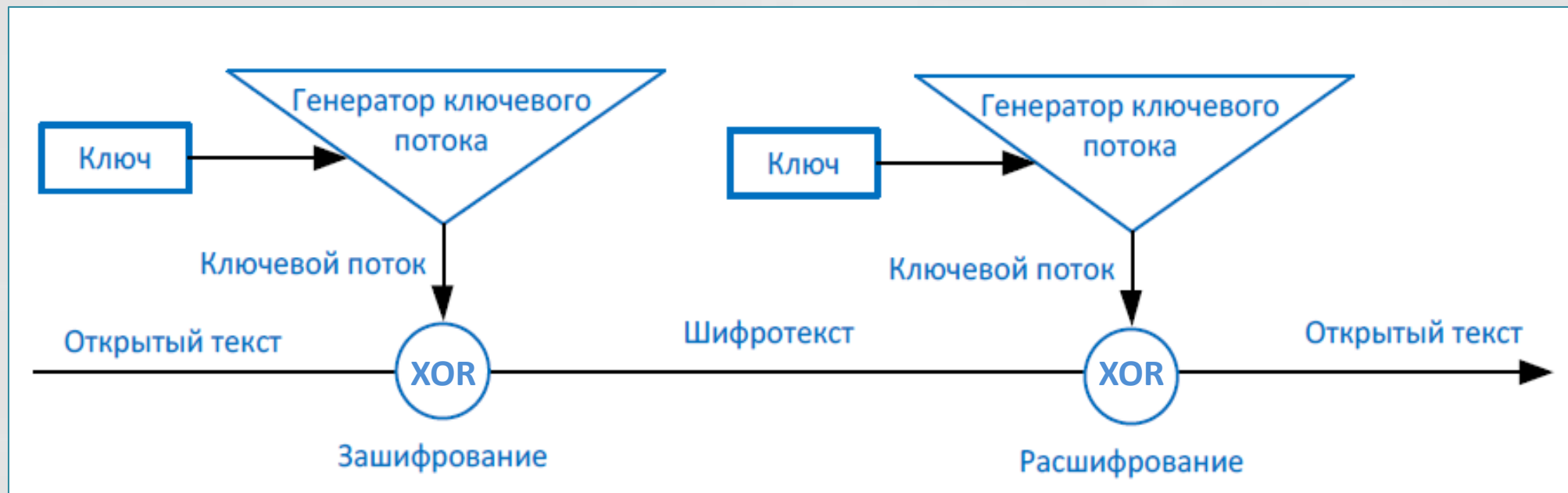
- Симметричные ключи (также называемые секретными ключами (*secret key*) - имеет двойную функциональность и применяется для зашифрования и для расшифрования
- Каждый из абонентов должен хранить ключ в секрете и надлежащим образом защищать его
- Поскольку оба абонента используют один и тот же ключ, то 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)..

# 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

Абонент Е (Ева) – противник, конкурент

Криптоаналитик



Открытый канал связи

Открытый  
текст



Зашифров  
ание



Шифро  
текст



Расшифро  
вание



Открытый  
текст

Абонент А (Алиса) -  
отправитель



Абонент Б (Боб) -  
получатель

# 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

Абонент Е (Ева) – противник, конкурент

Криптоаналитик



Открытый канал связи

Открытый  
текст

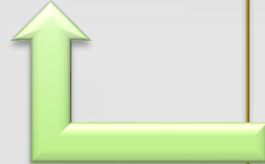
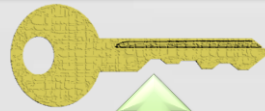
Зашифров  
ание

Шифро  
текст

Расшифро  
вание

Открытый  
текст

Абонент А (Алиса) -  
отправитель

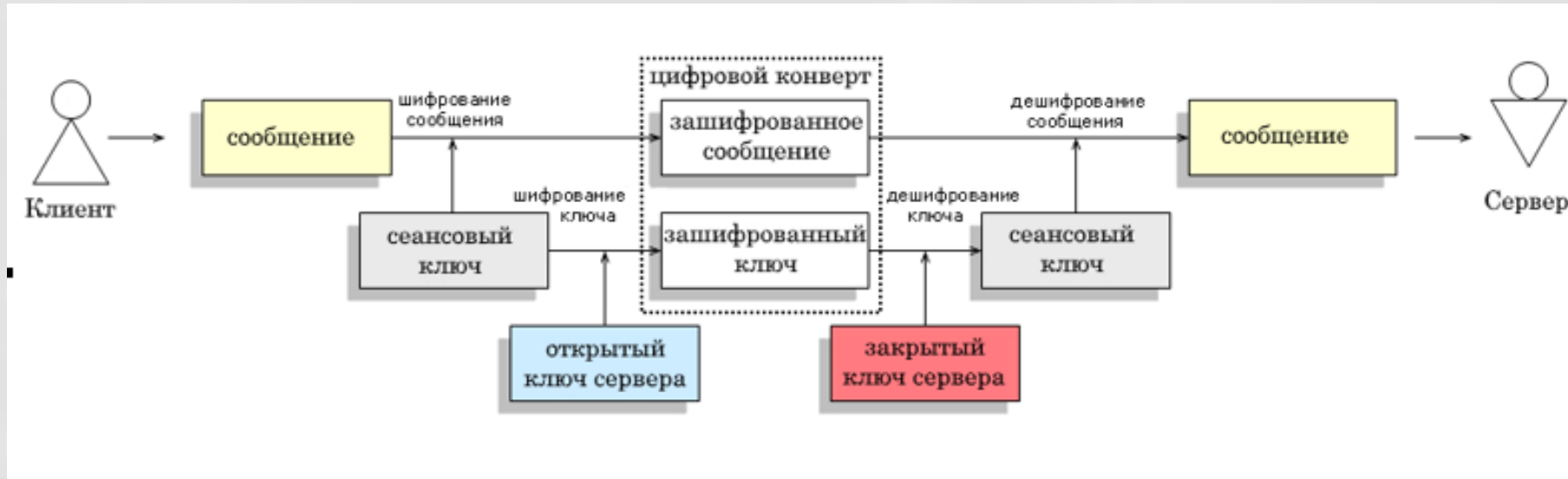


Асимметричный  
криптографический  
протокол



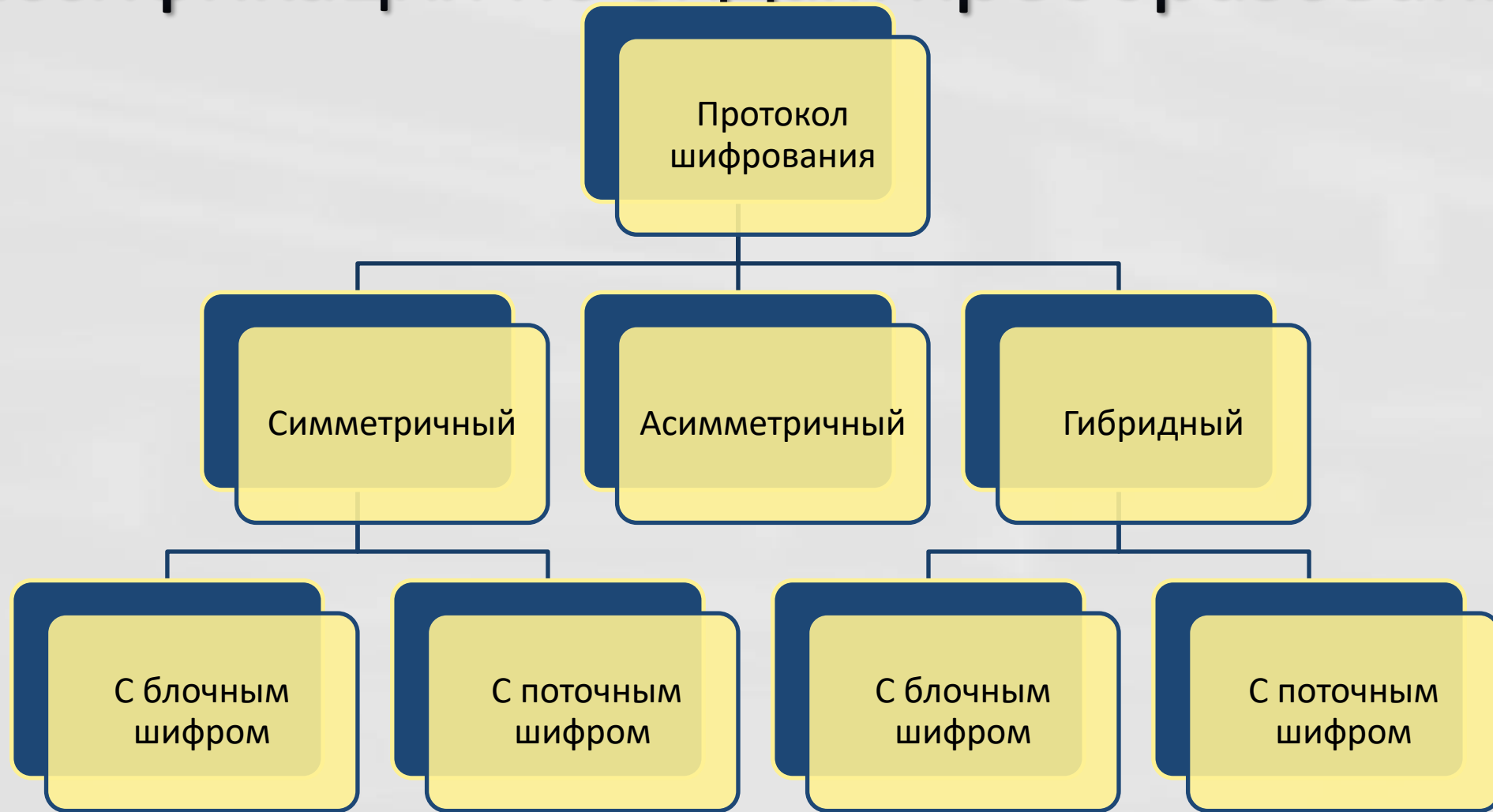
Абонент Б (Боб) -  
получатель

# Пример гибридного шифрования на основе асимметричного шифра



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

# Классификация по видам преобразований



# Классификация по видам криптостойкости

