Технология защищенного документооборота

Лекция 2 - Криптография

Криптография

Криптография - это наука об обеспечении безопасности данных. Она занимается поисками решений четырех важных проблем безопасности:

- ***конфиденциальности*** - когда нужно передать данные так, чтобы человек, перехвативший зашифрованное сообщение, не смог узнать его содержание;
- ***аутентификации*** - получатель сообщения хочет быть уверен, что оно пришло от определённой стороны, а не от кого-либо ещё;
- ***целостности*** - получатель сообщения хочет доказательства того, что оно не было изменено третьей стороной;
- ***контроль участников взаимодействия.***

Криптографическая стойкость

Криптографическая стойкость (или криптостойкость) — способность криптографического алгоритма противостоять возможным атакам на него. Атакующие криптографический алгоритм используют методы криптоанализа. Стойким считается алгоритм, который для успешной атаки требует от противника недостижимых вычислительных ресурсов, недостижимого объёма перехваченных открытых и зашифрованных сообщений или же такого времени раскрытия, что по его истечению защищенная информация будет уже не актуальна, и т. д.

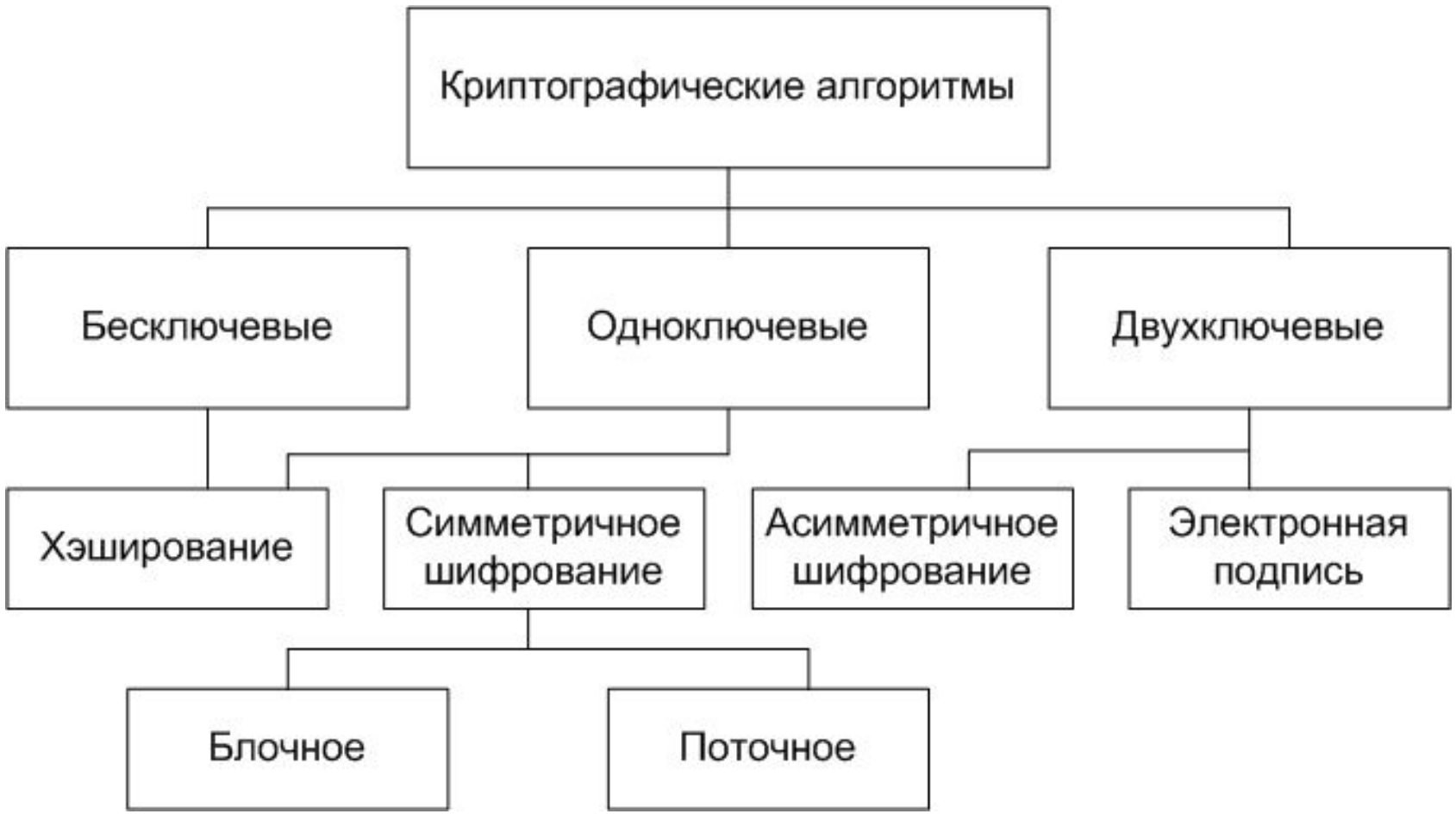
Современная криптография

- симметричные криптосистемы;
- асимметричные криптосистемы;
- системы электронной цифровой подписи (ЭЦП);
- хеш-функции;
- управление ключами;
- получение скрытой информации;
- квантовую криптографию.

Шифрование

Шифрование - это преобразование данных в нечитабельную форму, используя ключи шифрования-расшифровки. Шифрование позволяет обеспечить конфиденциальность, сохраняя информацию в тайне от того, кому она не предназначена.

Классификация



Виды шифров

Блочный шифр — оперирующего группами бит фиксированной длины — блоками, характерный размер которых меняется в пределах 64–256 бит. Если исходный текст (или его остаток) меньше размера блока, перед шифрованием его дополняют.

Поточный шифр (stream cipher) - выполняет преобразование входного сообщения по одному биту (или байту) за операцию. Поточный алгоритм шифрования устраняет необходимость разбивать сообщение на целое число блоков достаточно большой длины, следовательно, он может работать в реальном времени. Таким образом, если передается поток символов, каждый символ может шифроваться и передаваться сразу.

Симметричное шифрование

Способ шифрования, в котором для шифрования и дешифрования применяется один и тот же криптографический ключ. Ключ алгоритма должен сохраняться в тайне обеими сторонами, алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Симметричное шифрование

Достоинства

- скорость
- простота реализации (за счёт более простых операций)
- меньшая требуемая длина ключа для сопоставимой стойкости

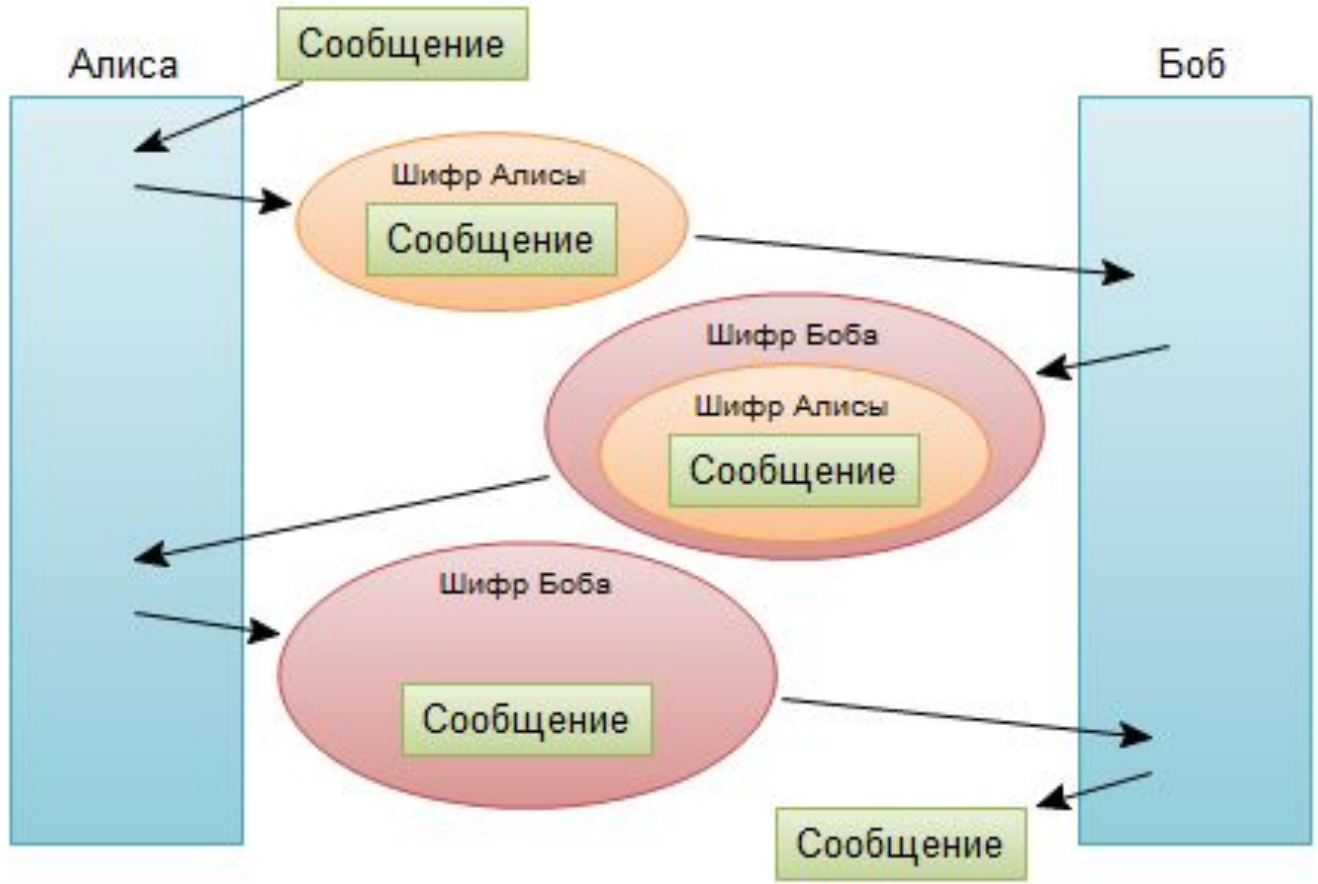
Недостатки

- сложность управления ключами в большой сети
- сложность обмена ключами

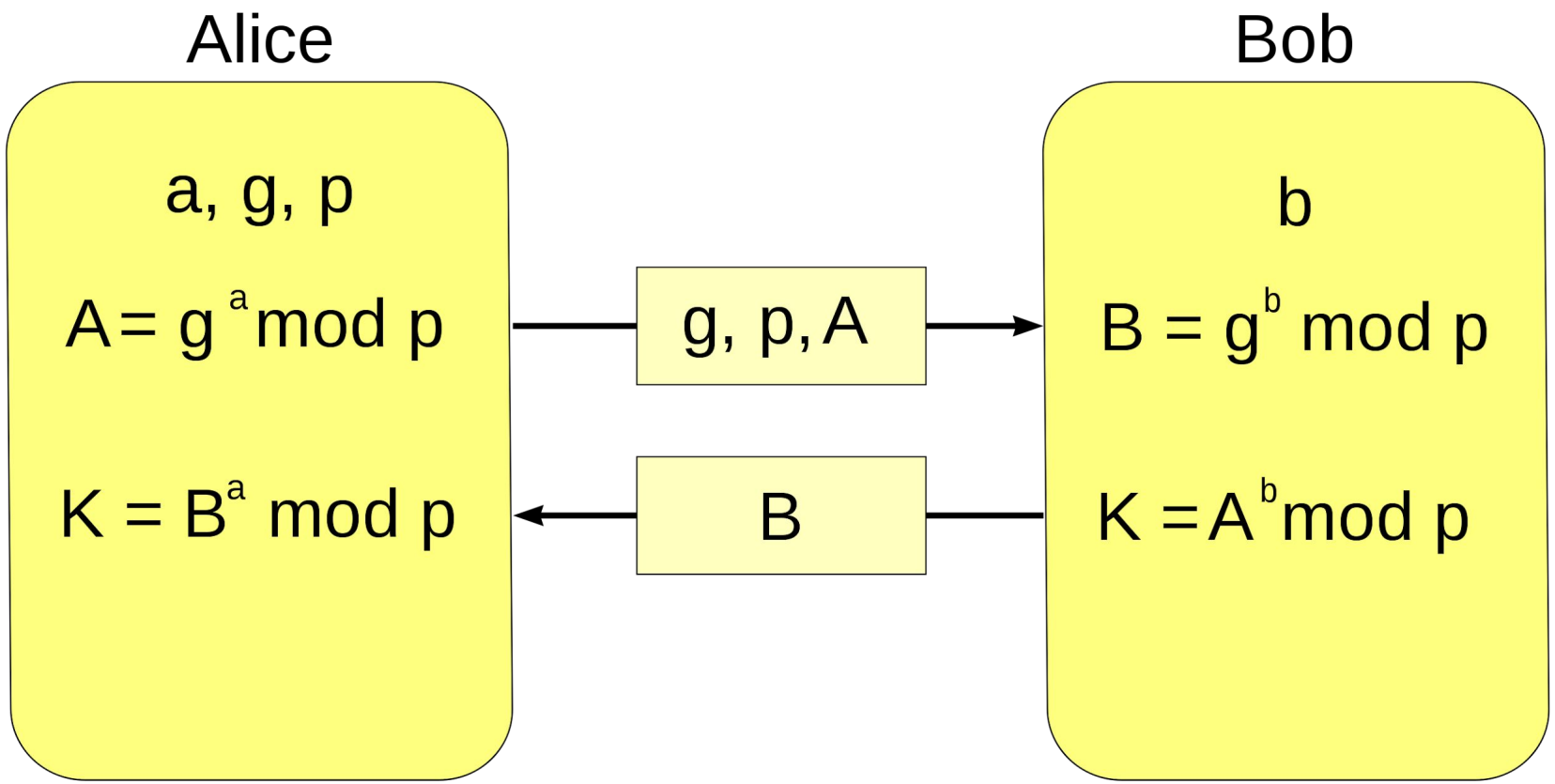
Ассиметричное шифрование

Это метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом. Открытый и закрытый ключи — это очень большие числа, связанные друг с другом определенной функцией, но так, что, зная одно, крайне сложно вычислить второе.

Шифрование с открытым ключом



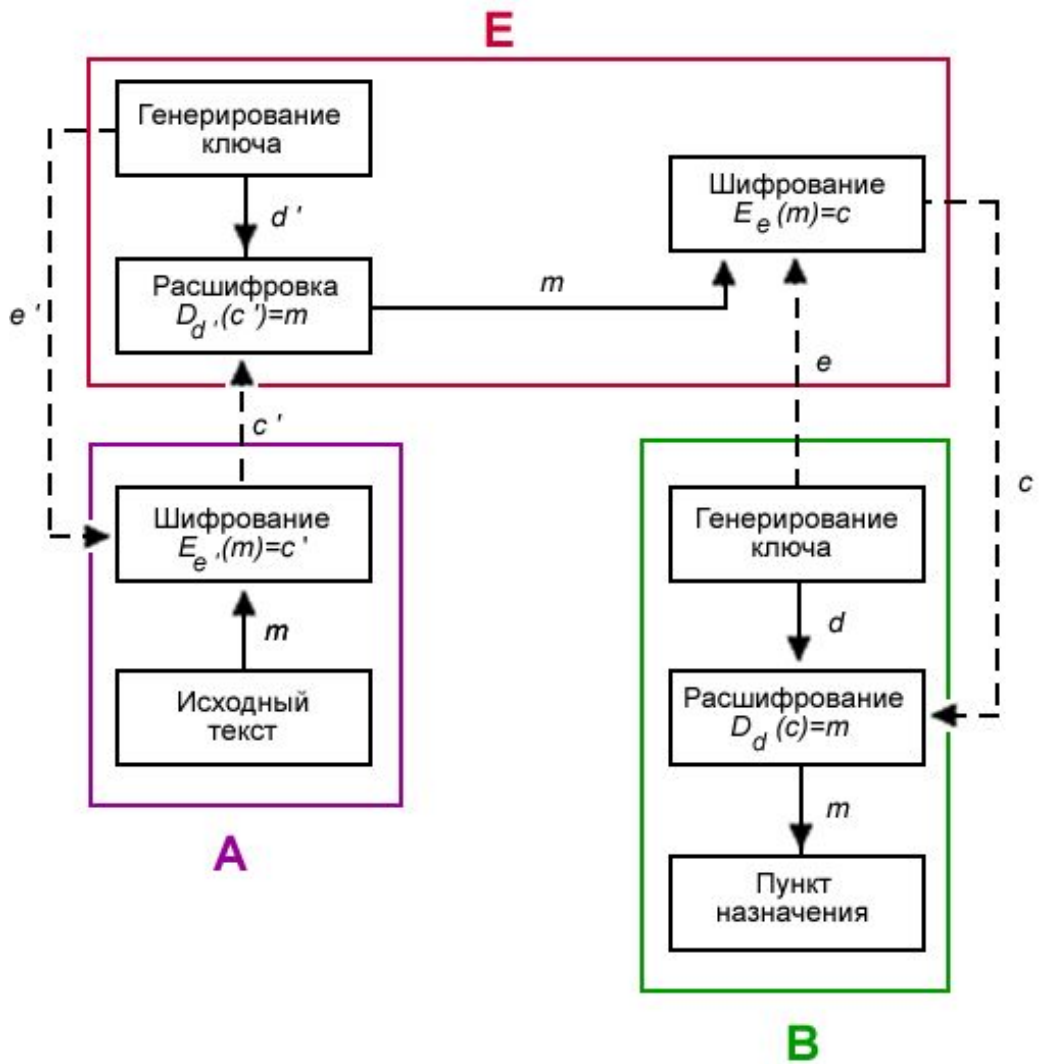
Алгоритм Диффи — Хеллмана



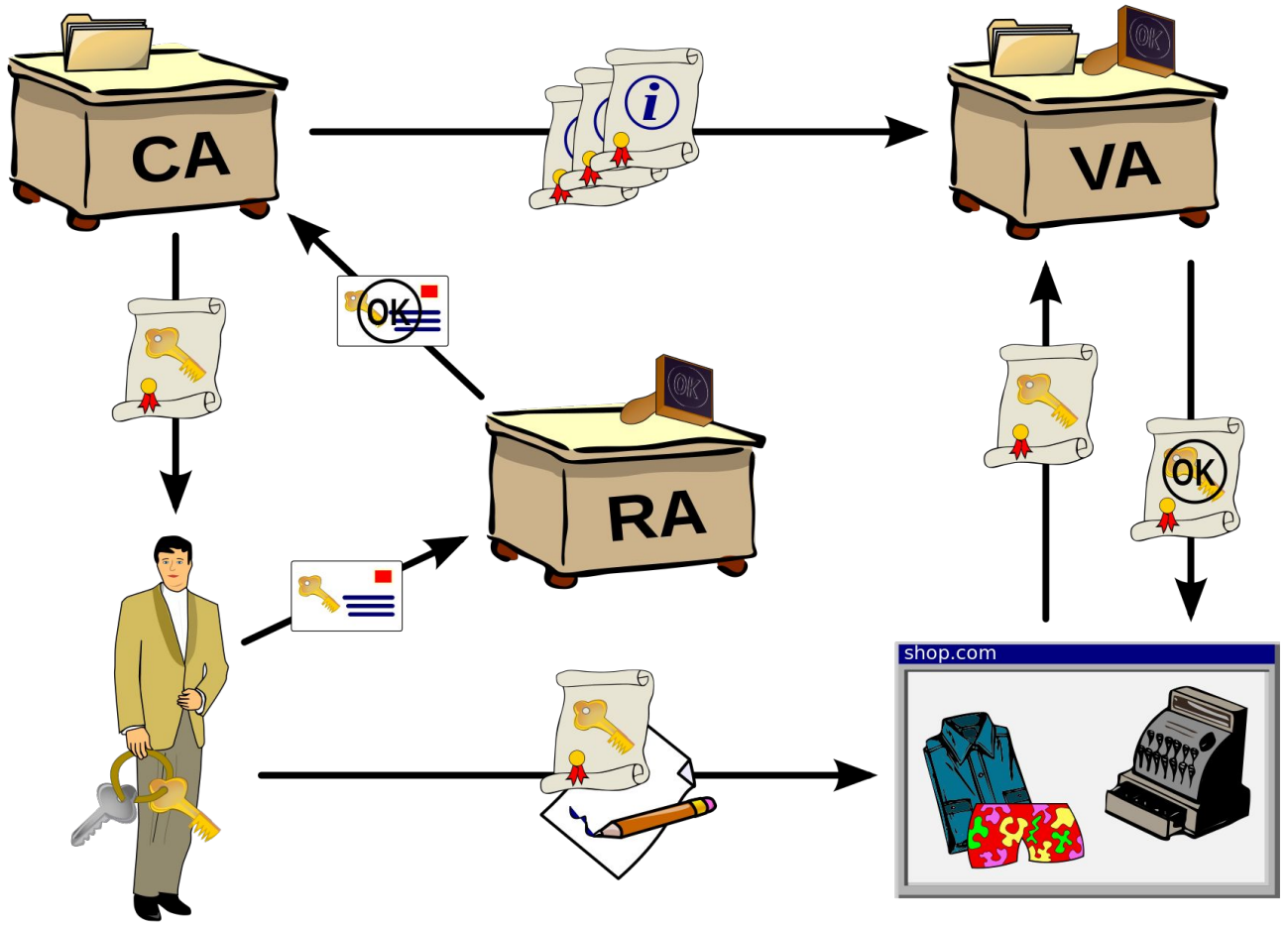
$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Асимметричное шифрование

Проблемы АШ


E
Генерирование ключа
d '
Расшифровка $D_{d'}(c')=m$
m
Шифрование $E_e(m)=c$
e '
e
c '
c
Шифрование $E_{e'}(m)=c'$
m
Исходный текст
A
Генерирование ключа
d
Расшифрование $D_d(c)=m$
m
Пункт назначения
B

PKI - Public Key Infrastructure



Стандарт X.509

Это набор стандартных полей, содержащих сведения о пользователе или устройстве, и их соответствующий открытый ключ. Стардарт X.509 определяет, какие сведения входят в сертификат и как они кодируются

Сертификат X.509