Электронная коммерция

Обеспечение безопасности в сети Интернет

Вопросы темы:

1. Шифрование. Алгоритмы шифрования.

2. Симметричное шифрование.

3. Ассиметричное шифрование.

4. Цифровой сертификат. Электронно-цифровая подпись.

5. Протокол SSL

Вопрос 1.

Шифрование. Алгоритмы шифрования.

Информационная безопасность(по законодательству РФ) - состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Информационная безопасность имеет три основные составляющие:

1. конфиденциальность - защита чувствительной информации от несанкционированного доступа;
2. целостность - защита точности и полноты информации и программного обеспечения;
3. доступность - обеспечение доступности информации и основных услуг для пользователя в нужное для него время;

А так же:

4. достоверность;
5. сохранность.

Шифрование

Шифрование – такое преобразование элементов информации, после которого восстановление исходной информации становится исключительно трудным для всех, кроме лица, которому предназначается информация.

– зашифрование - процесс преобразования открытых данных в зашифрованные данные при помощи шифра.

– расшифрование - процесс преобразования зашифрованных данных в открытые данные при помощи шифра.

История криптографии

Криптография - ровесница истории человеческого языка.

Первоначально письменность, сама по себе, была криптографической системой, так как в древних обществах ею владели только избранные.

Первые действительно достоверные сведения с описанием метода шифрования относятся к периоду смены старой и новой эры и описывают шифр Цезаря: в нем каждая буква сообщения заменялась на третью следующую за ней в алфавитном порядке букву

История криптографии

Бурное развитие криптографические системы получили в годы первой и второй мировых войн.

Немецким инженером Артуром Шербиусом была изобретена и запатентована шифровальная электромеханическая машина «Энигма» вскоре после окончания первой мировой войны

Правило Керкхоффа

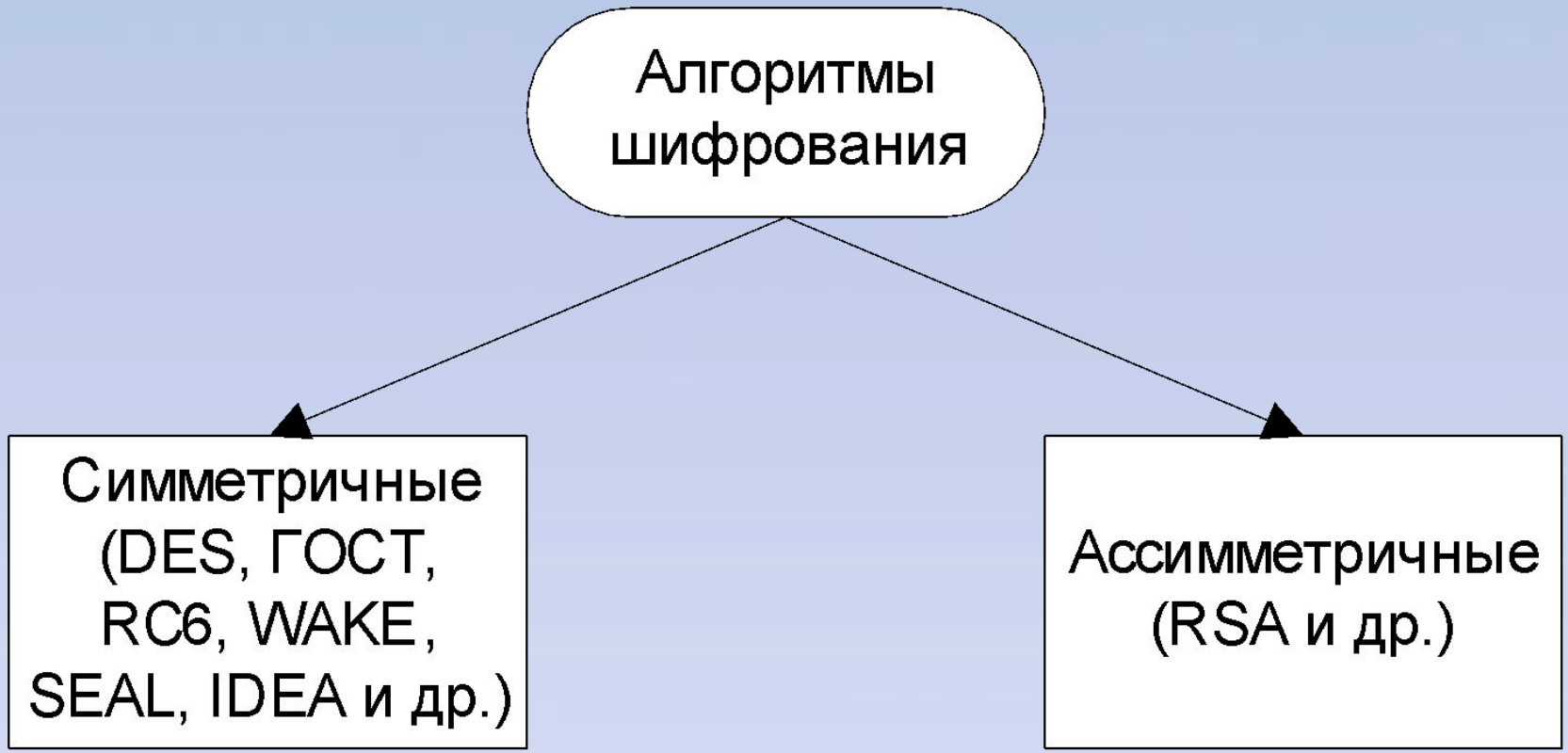
Существует общее правило, сформулированное в позапрошлом веке голландским ученым Ф. Керкхоффом (1835-1903):

Стойкость шифра должна быть обеспечена в том случае, когда известен весь алгоритм зашифровывания, за исключением секретного ключа

Основные понятия криптографии

- Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования сообщений.
- Алгоритм – последовательность действий по преобразованию исходного сообщения в зашифрованное или наоборот, использующая ключ(и) шифрования.
- Пространство ключей – набор возможных значений ключа.

Классы алгоритмов шифрования



Вопрос 2.

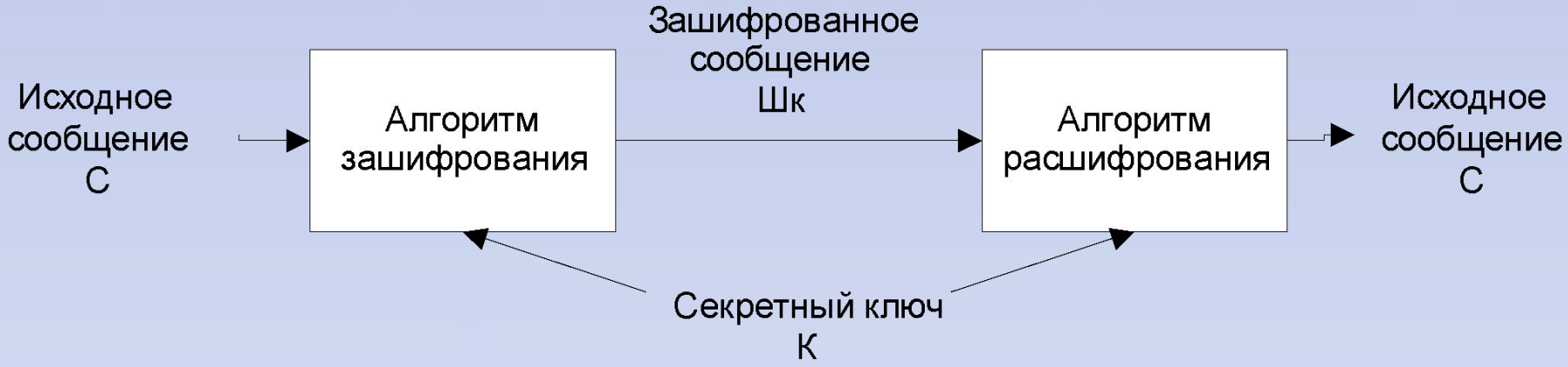
Симметричное шифрование

Симметричные алгоритмы

Симметричными являются алгоритмы, в которых для зашифрования и расшифрования используется один и тот же секретный ключ.

Чтобы начать использовать систему, необходимо получить общий секретный ключ так, чтобы исключить к нему доступ злоумышленника.

Общая схема симметричных алгоритмов



Симметричные алгоритмы подразделяются на:

- Поточные (сообщение шифруется побитно от начала и до конца)
- Блочные (сообщение разбивается на блоки и шифруется поблочно)

Основные действия в симметричных алгоритмах

- подстановки;
- перестановки;
- гаммирование;

Алгоритм DES

Алгоритм был разработан в 1977 году, в 1980 году был принят NIST (National Institute of Standards and Technolody США) в качестве стандарта (FIPS PUB 46).

Данные шифруются 64-битными блоками, используя 56-битный ключ. Алгоритм преобразует за несколько раундов 64-битный вход в 64-битный выход. Длина ключа равна 56 битам.

Алгоритм IDEA

IDEA (International Data Encryption Algorithm) является блочным симметричным алгоритмом шифрования, разработанным Сюдзя Лай (Xuejia Lai) и Джеймсом Массей (James Massey) в 1990 году.

Алгоритм IDEA

IDEA является блочным алгоритмом, который использует 128-битовый ключ для шифрования данных блоками по 64 бита.

Криптографическую стойкость IDEA характеризуют:

1. Длина блока: в 64 бита в 90-е годы означало достаточную силу.
2. Длина ключа: 128 бит IDEA считается достаточно безопасным.
3. Конфузия: зашифрованный текст должен зависеть от ключа сложным и запутанным способом.
4. Диффузия: каждый бит незашифрованного текста должен влиять на каждый бит зашифрованного текста

Алгоритм ГОСТ 28147

Алгоритм ГОСТ 28147 является отечественным стандартом для алгоритмов симметричного шифрования. ГОСТ 28147 разработан в 1989 году, является блочным алгоритмом шифрования, длина блока равна 64 битам, длина ключа равна 256 битам, количество раундов равно 32.

Другие симметричные алгоритмы

- Triple DES. Это усовершенствованный вариант DES, применяющий для шифрования алгоритм DES три раза с разными ключами. Он значительно устойчивее к взлому, чем DES;
- Skipjack. Алгоритм создан и используется Агентством национальной безопасности США. Длина ключа 80 бит. Шифрование и дешифрование информации производится циклически (32 цикла);
- RC4. Он использует ключ переменной длины (в зависимости от необходимой степени защиты информации) и работает значительно быстрее других алгоритмов. RC4 относится к так называемым потоковым шифрам.

Основные преимущества симметричных алгоритмов

- высокая скорость зашифрования \ расшифрования;
- возможность работы на больших объёмах и потоках информации;
- менее требовательны к вычислительным ресурсам системы.

Основные недостатки симметричных алгоритмов

- сложность распространения ключа между участниками;
- сложность сохранения ключа в тайне при большом количестве участников;
- меньшая стойкость в взлому;
- сложность реализации самих алгоритмов ввиду многоэтапности;
- отправитель, и получатель информации владеют одним и тем же ключом, что делает невозможным аутентификацию отправителя.

Длина ключей

- Ключ 56 бит – это 2^{56} комбинаций ключей. При скорости перебора – 1млн. ключей в секунду потребуется 2000 лет.
- Ключ 64 бита – 600.000 лет
- Ключ 2048 бит – 10^{197} лет. (вселенная существует только 10^{10} лет)

Длина ключей

Вид сообщений	Жизненный интервал	Минимальная длина ключа
Тактическая военная информация	Мин/часы	56 бит
Сообщения о продуктах, слияниях компаний и т.д.	Дни/недели	56-64 бит
Торговые секреты (рецепт Coca Cola)	Декады	64 бита
Секреты водородной бомбы	>40 лет	128 бит
Дипломатические взаимоотношения	>65 лет	минимум 128 бит
Результаты переписи населения	100 лет	Как минимум 128 бит

Вопрос 3.

Ассиметричное шифрование

В ассиметричных алгоритмах используются два ключа - открытый и закрытый (секретный), которые математически связаны друг с другом.

Ключи

- Открытый ключ – число, которое свободно может передаваться по открытым каналам и не является секретом
- Закрытый ключ – число, никогда не передающееся по каналам связи, хранящееся только у владельца и являющееся его секретом.
- Генерация пары ключей должна происходить обязательно одновременно

Схемы использования

Исходное состояние:

Участник А:

- открытый ключ Оа;
- закрытый ключ За;
- открытый ключ Об;
- сообщение С.

Участник Б:

- открытый ключ Об;
- закрытый ключ Зб;
- открытый ключ Оа.

Схема 1 – отправка сообщения только участнику Б

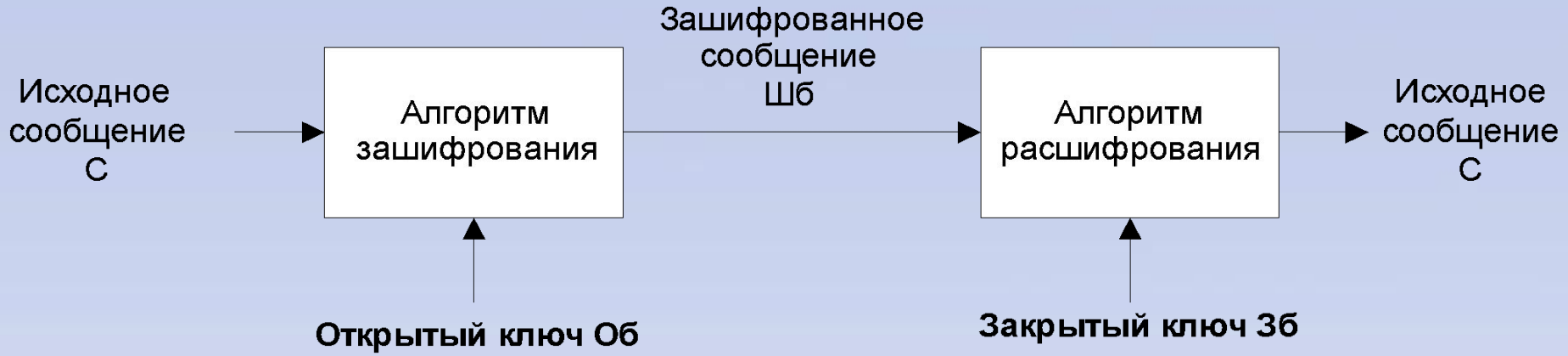
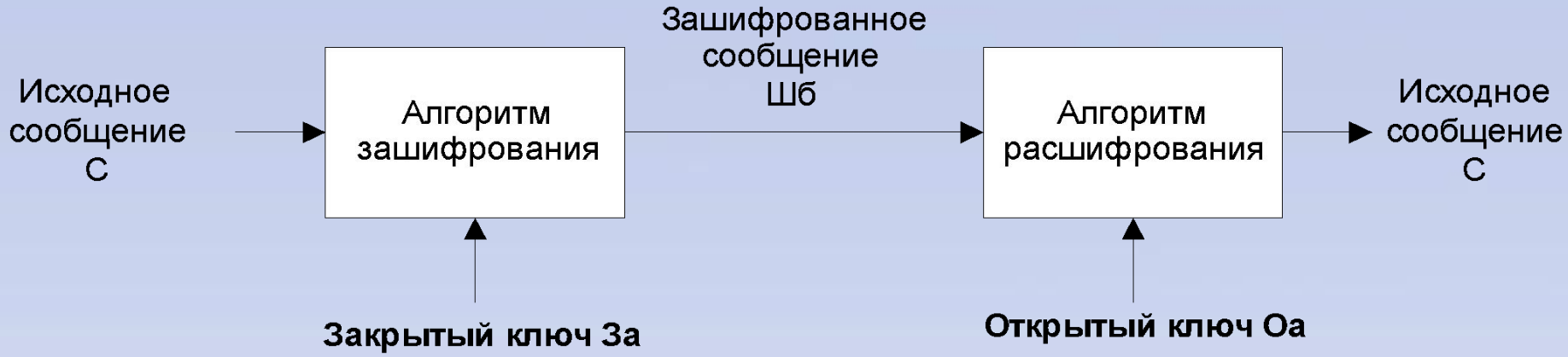


Схема 2 – подтверждение, что сообщение отправил участник А



Авторы

Концепция шифрования по общему ключу изобретена Уитфилдом Диффи и Мартином Хеллманом в 1977г.

Чуть позже другая группа ученых - Рон Ривест и Ади Шамир, в области компьютерных наук, стали использовать разложение произведений простых чисел на множители как часть того, что теперь известно под названием криптосистема RSA

Основные преимущества асимметричных алгоритмов

- отсутствие необходимости в секретном канале для передачи ключей;
- секретный ключ никогда не передаётся;
- может использоваться для организации секретного канала по передаче ключа для симметричного алгоритма;
- большая сложность во взломе сообщения.

Основные недостатки асимметричных алгоритмов

- большая вычислительная сложность для зашифрования\расшифрования;
- возможность использования только для небольших объёмов информации;
- сильная зависимость времени работы алгоритма от длины ключа.

Вопрос 4.

Цифровой сертификат. Электронно-цифровая подпись

Цифровой сертификат

Цифровой сертификат – электронный документ, выданный и заверенный удостоверяющим центром.

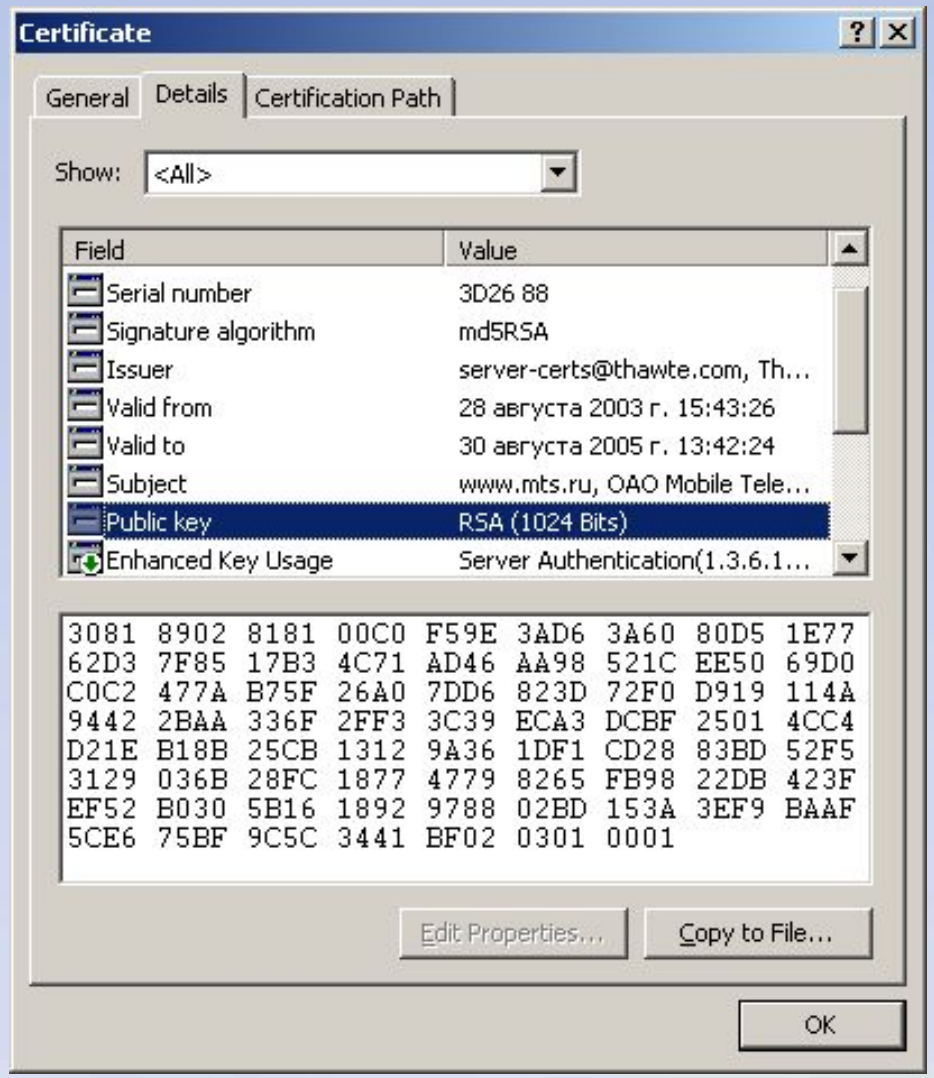
Цифровой сертификат можно рассматривать как электронное удостоверение пользователя по аналогии с традиционным удостоверением (паспортом), которое позволяет удостовериться в том, что при обмене электронными документами Вы имеете дело с определённым лицом.

Цифровой сертификат

По своей сути цифровой сертификат - это небольшой файл, содержащий в себе следующую информацию:

- имя и идентификатор владельца сертификата;
- открытый ключ;
- имя, идентификатор и цифровую подпись удостоверяющего центра;
- серийный номер, версию и срок действия сертификата.

Цифровой сертификат



Этапы получения цифрового сертификата

1. Генерация пары взаимосвязанных ключей (открытый и закрытый)
2. Создание запроса на генерацию сертификата (Certificate Request)
   a. имя и идентификатор владельца сертификата;
   b. открытый ключ;
   c. цели использования;
   d. доп. Информация;
3. Передача запроса и открытого ключа удостоверяющему центру
4. Генерация сертификата с занесением в реестр сертификатов УЦ
5. Передача сертификата владельцу

Цифровой сертификат

Таким образом цель создания цифрового сертификата – сопоставить открытый ключ (обычное число) и понятное человеку «имя владельца», при котором достоверность такого сопоставления подтверждается третьей стороной.

Понятие ЭЦП

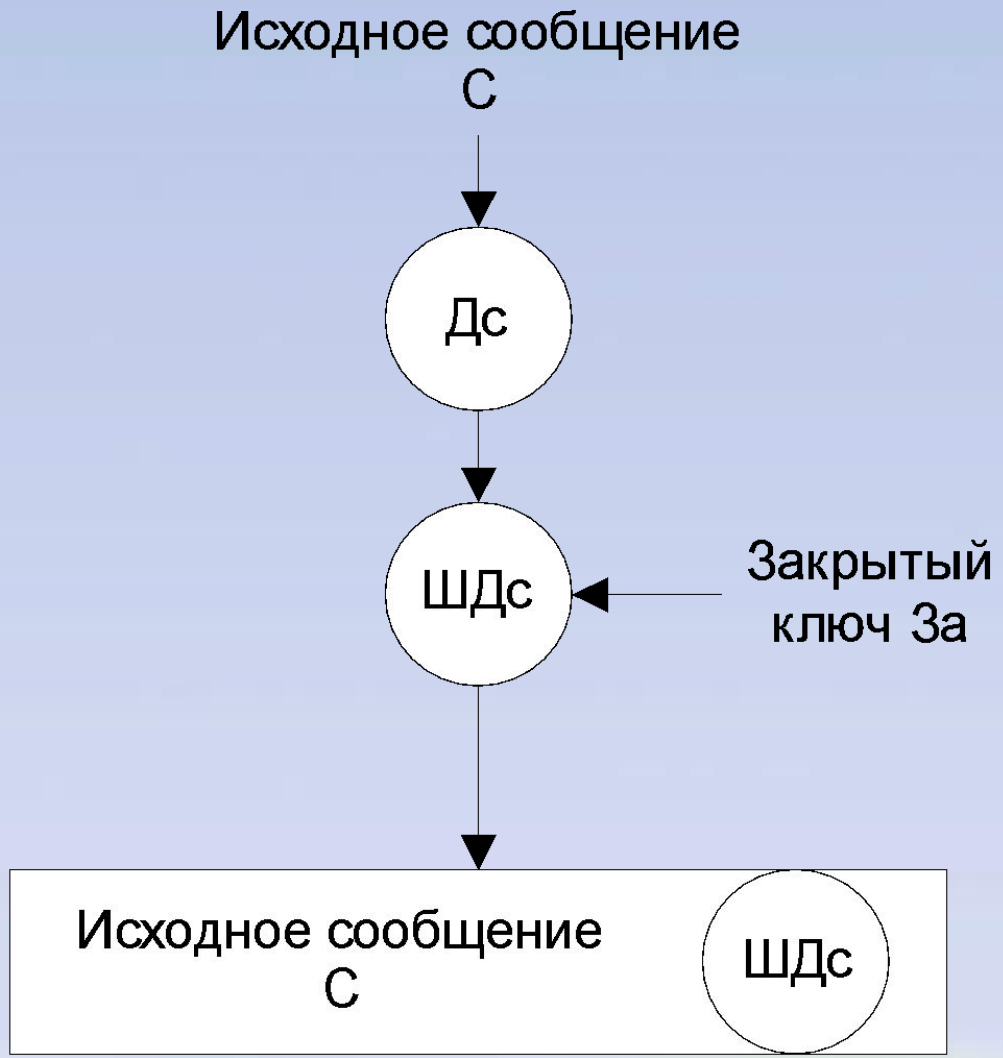
Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

ХЭШ функция

Хэш-функция — это процедура обработки сообщения, в результате действия которой формируется строка символов (дайджест сообщения) фиксированного размера.

Малейшие изменения в тексте сообщения приводят к изменению дайджеста при обработке сообщения хэш-функцией. Таким образом, любые искажения, внесенные в текст сообщения, отразятся в дайджесте.

Схема формирования ЭЦП



Для проверки ЭЦП необходимо

- Исходное сообщение С;
- Открытый ключ отправителя Оа;
- Дайджест сообщения Дс;
- Значение ЭЦП – ШДс.

В случае отрицательного результата возможны следующие причины:

- в электронный документ были внесены несанкционированные изменения;
- подпись для электронного документа была подделана;
- автором документа является другое лицо.

Вопрос 5.

Протокол SSL

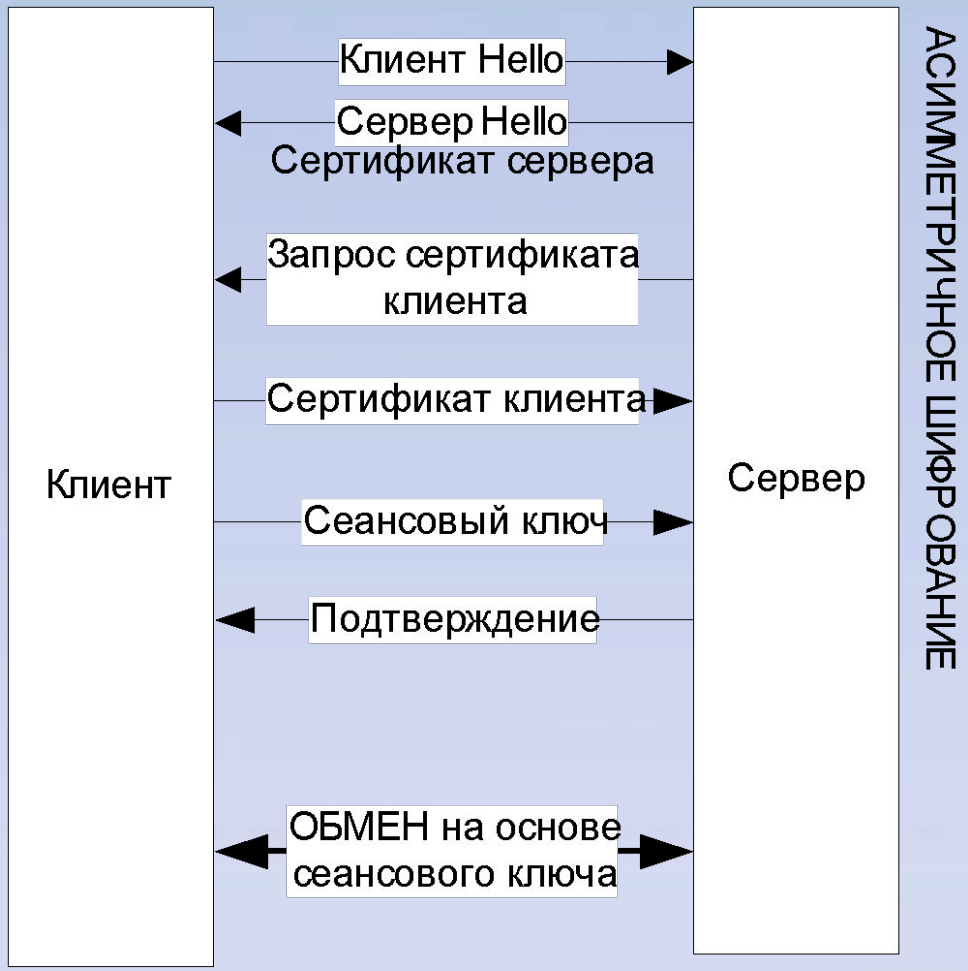
Протокол SSL

Протокол SSL (Secure Socket Layer) используется для защиты данных, передаваемых через Интернет. Он основан на комбинации алгоритмов асимметричного и симметричного шифрования.

Протокол SSL может работать в трех режимах:

1. при взаимной аутентификации сторон;
2. при аутентификации сервера и анонимности клиента;
3. при взаимной анонимности сторон.

Упрощённая схема работы протокола SSL



Возможные ошибки при установлении соединения

- Не поддерживается алгоритм шифрования;
- Не представлен сертификат;
- Представлен неверный сертификат;
- Неподдерживаемый тип сертификата.

Основные преимущества использования протокола SSL

- Функционирует на транспортном уровне и может быть использован вместе с любыми прикладными протоколами;
- Универсальность в использовании – является стандартом де-факто и поддерживается большинством клиентского и серверного ПО;
- Имеет возможность работать в 3х режимах;
- Совмещает стойкость асимметричного шифрования и скорость симметричного.

Основные недостатки использования протокола SSL

- Требует дополнительного обмена информацией и затрат времени на установление каждого соединения;
- Требует получения серверного сертификата;
- Осуществляется лишь защита соединения;
- Большинство ПО позволяет работать лишь с 40-битным ключом DES и 512-битным – RSA.