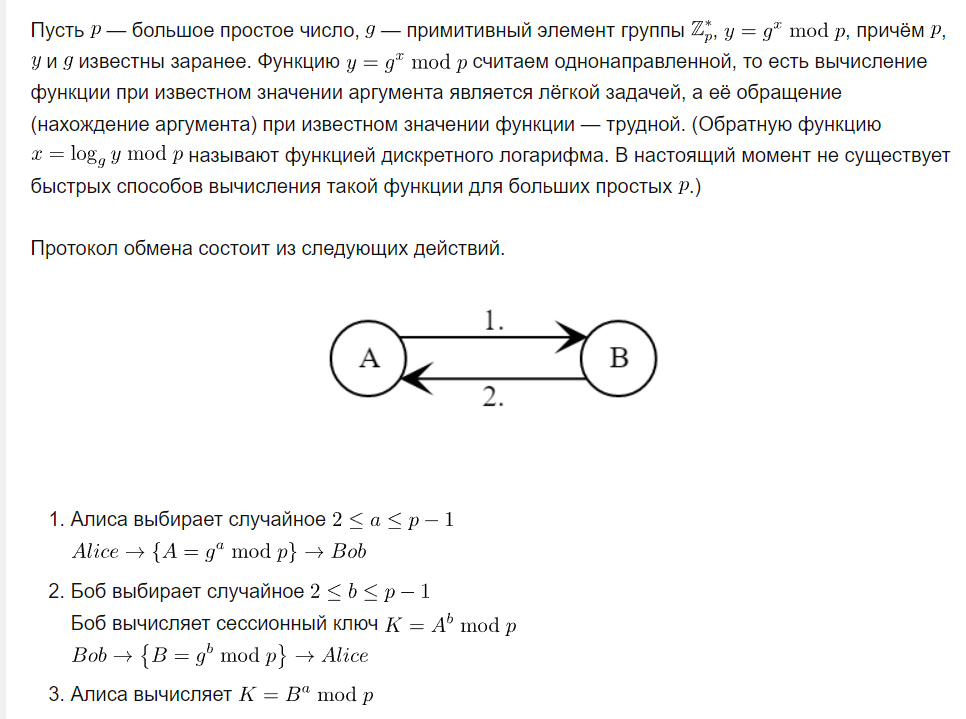
# Лабораторная 26

Диффи-Хелман



**ЭЦП**

В общем случае для формирования подписи некоторого сообщения отправитель шифрует дайджест(результат преобразования входного сообщения произвольной длины в выходную битовую строку фиксированной длины) этого сообщения своим секретным ключом и отправляет подпись вместе с сообщением. Получатель расшифровывает подпись открытым ключом отправителя и сравнивает результат расшифрования подписи с дайджестом принятого сообщения. Если два дайджеста совпадают, то подпись является подлинной.

## 1. Что такое хеш-функция?

***Хеш-функция*** – математическая или иная функция которая принимает на входе строку символов переменной (произвольной) длины и преобразует ее в выходную строку фиксированной (обычно – меньшей) длины

## 2. Что такое хеширование?

***Хеширование*** (или хэширование, англ. hashing ) – это преобразование входного массива данных определенного типа и произвольной длины в выходную битовую строку фиксированной длины.

## 3. Перечислите алгоритмы хеширования.

***Алгоритмы CRC16/32*** — контрольная сумма (не криптографическое преобразование)

***Алгоритмы MD2/4/5/6***

***Алгоритмы SHA0/1/2/224/256/384/512/3***

Российский стандарт — ***ГОСТ 34.11-94***

## 4. Поясните понятие «сеансовый ключ»

***Сеансовые ключи*** — ключевая информация в криптографии, вырабатываемая между двумя пользователями, обычно для защиты канала связи.

## 5. Поясните понятия «публичный» и «секретный» ключи?

***Открытый*** (публичный ключ) доступен всем. Используется для шифрования данных при обращении браузера к серверу.

***Закрытый*** (секретный ключ) известен только владельцу сайта. Используется для расшифровки данных, отправленных браузером.

## 6. Поясните понятие «дайджест».

**Хеш-сумма**, также называемая **дайджестом** — результат преобразования входного сообщения произвольной длины в выходную битовую строку фиксированной длины.

## 7. Для чего используется дайджест.

Значение хеш-суммы может использоваться для проверки целостности данных, их идентификации и поиска, а также заменять собой данные, которые небезопасно хранить в явном виде (например, пароли, ответы на вопросы тестов и т. д.). Также алгоритмы хеширования используются для проверки целостности и подлинности файлов.

## 8. Поясните принцип работы алгоритма Диффи-Хеллмана.

Протокол Диффи—Хеллмана — [криптографический протокол](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB), позволяющий двум и более сторонам получить общий секретный [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)), используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов [симметричного шифрования](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5).

При работе алгоритма, каждая сторона:

1. генерирует случайное натуральное число a — *закрытый ключ*
2. совместно с удалённой стороной устанавливает *открытые параметры p и g* (обычно значения p и g генерируются на одной стороне и передаются другой), где  
   p является случайным простым числом  
   g является первообразным корнем по модулю p
3. вычисляет открытый ключ A, используя преобразование над закрытым ключом  
   A = ga mod p
4. обменивается открытыми ключами с удалённой стороной
5. вычисляет общий секретный ключ K, используя открытый ключ удаленной стороны B и свой закрытый ключ a  
   K = Ba mod p  
   К получается равным с обоих сторон, потому что:  
   Ba mod p = (gb mod p)a mod p = gab mod p = (ga mod p)b mod p = Ab mod p

В практических реализациях, для a и b используются числа порядка 10100 и p порядка 10300. Число g не обязано быть большим и обычно имеет значение в пределах первого десятка.

## 9. Поясните понятие «цифровая подпись», объясните принцип ее применения.

***Электронная цифровая подпись (ЭЦП)*** — уникальная комбинация знаков или паролей, которая служит аналогом собственноручной подписи на бумаге. Проще говоря, цифровая подпись позволяет сделать документы в электронном виде юридически значимыми и защитить их от подделки.

Электронная подпись работает по ассиметричному принципу шифрования. То есть документ зашифровывается с помощью закрытого ключа, а расшифровывается с помощью открытого.

Подписание документа производится в несколько этапов:

1. Хеш документа шифруется с помощью закрытого ключа.
2. Полученная подпись добавляется к документу.
3. К документу прикрепляется сертификат проверки.

# Лабораторная 27

## 1. Что такое WebDav?

**WebDAV** — набор расширений и дополнений к протоколу HTTP, поддерживающих совместную работу пользователей над редактированием файлов и управление файлами на удаленных веб-серверах

## 2. Назначение WebDav.

определяет, основные функции работы с файлами, такие как копирование, перемещение, удаление и создание, выполняются они с помощью протокола HTTP

## 3. Перечислите основные функции WebDav.

Выполнение основных файловых операций над объектами на удаленном сервере;

Выполнение расширенных файловых операций (блокировки, поддержка версий);

Работа с любым типом объектов (не только файлы);

Поддержка метаданных (свойств) объектов;

Поддержка одновременной работы над объектами.

## 4. Назовите несколько методов WebDav, расширяющих методы протокола HTTP.

**copyFile** - Скопируйте файл из одного места в другое.

**createDirectory** - Создайте новый каталог

**createReadStream** - Синхронно создать читаемый поток для удаленного файла

**createWriteStream** - Создайте поток записи, нацеленный на удаленный файл

**customRequest** - Пользовательские запросы

**deleteFile** - удаление файла

**exists** - Проверьте, существует ли файл или каталог.

