**Лабораторная работа 23**

**ПСКП, ПОИТ-3**

**Задание 01**

1. Разработайте клиент-серверное приложение 23-01( 21-01s – server (EXPRESS), 21-01c – клиент).
2. При подключении клиента (GET/), сервер предлагает клиенту по схеме Диффи-Хеллмана (ДХ) вычислить сеансовый ключ, для симметричного шифрования. Схему (протокол) обмена данными в ходе вычисления ключа разработайте самостоятельно.
3. В случае нарушения схемы обмена данными, в ходе схемы ДХ, сервер генерирует ответ с кодом 409.
4. После вычисления ключа, сервер высылает по запросу (GET /resource) зашифрованный txt-файл, содержащий имя, фамилию и отчество студента.
5. Клиент, получив от сервера зашифрованный файл, расшифровывает его и записывает на диск клиента.

**Задание 02**

1. Разработайте клиент-серверное приложение 23-02( 21-02s – server (EXPRESS), 21-02c – клиент).
2. В результате, разработанной вами схемы (протокола) обмена данными, клиент должен получить от сервера txt-файл, содержащий имя, фамилию и отчество студента (в открытом виде) и цифровую подпись к нему.
3. В случае нарушения схемы обмена данными, сервер генерирует ответ с кодом 409.
4. Клиент проверяет сообщение цифровую подпись и выводит сообщение в консоль с результатом проверки.

**Задание 03**. Ответьте на вопросы

1. Что такое хеш-функция?
2. Что такое хеширование?
3. Перечислите алгоритмы хеширования.
4. Поясните понятие «сеансовый ключ»
5. Поясните понятия «публичный» и «секретный» ключи?
6. Поясните понятие «дайджест».
7. Для чего используется дайджест.
8. Поясните принцип работы алгоритма Диффи-Хеллмана.
9. Поясните понятие «цифровая подпись», объясните принцип ее применения.
10. Что такое хеш-функция?

ф., вып. необратимые преобразования исх. текста в строку заданной длины

1. Что такое хеширование?

процесс преобр

1. Перечислите алгоритмы хеширования.

sha256, sha512, md5, md6

1. Поясните понятие «сеансовый ключ»

ключ, кот. вырабатываются между 2 пользователями канала защиты связи на t сеанса, исп. для защиты передачи зашифр. данных

1. Поясните понятия «публичный» и «секретный» ключи?

публ – исп для шифрования и все знают  
секр – для расшифр и знает только С

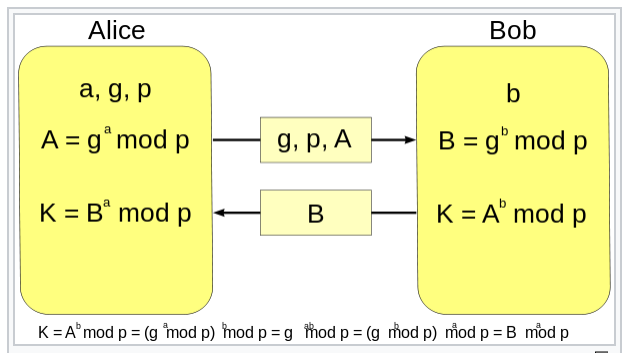
1. Поясните понятие «дайджест»

результат хэш-функции

1. Для чего используется дайджест.

исп для идентификации владельца, проверки что файл передан без ошибок, проверки контр.сумм

1. Поясните принцип работы алгоритма Диффи-Хеллмана.

  
есть С-К  
на С генер закр.ключ а + откр. числа g, p  
 вычисляем число А = ga mod p  
 передаем клиенту полученное А + g,p  
на К генер закр. ключ b  
 тоже вычисл число B = gbmod p, уже возводит в степень своего ключа……  
криптостойкость за счет того, что генер достаточно большие ключи a,b

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

цифр подпись – мы совершаем преобразование над к-то блоком данных, которое мы будем передавать вместе с этими данными, чтобы можно было удостовериться, что эти данные никак не изменены