**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?

Это функция которая выполняет необратимое преобразование исходного текста в строку заданной длины

1. Что такое хеширование?

Процесс преобразования, который происходит в хеш-функции

1. Перечислите алгоритмы хеширования.

Sha256, sha512, md5, md6

1. Поясните понятие «сеансовый ключ»

Ключ, который вырабатывается между 2 пользователями защиты канала связи на время сеанса и используется для защищенной передачи зашифрованных данных между друг другом.

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

Публичный – ключ, который используется для зашифрования и его все знают и используется для шифрования.

Секретный – знает только сервер и использует для расшифровки.

1. Поясните понятие «дайджест».

Это результат хеш-функции (строка которую получили)

1. Для чего используется дайджест.

Для идентификации владельца, проверки совпадений в файле, то что файл передан без ошибки, также используется как контрольная сумма в запросе

1. Поясните принцип работы алгоритма Диффи-Хеллмана.

Есть С и К.

На С генерируется секретный ключ число а, и числа г и п, которые открытые и мы будем их передавать.

С помощью а вычисляем число А = g^a mod p. И передаем это клиенту А, г и п.

К генерирует свой закрытый ключ б. И также вычисляет Б = g^b mod p. И также передает это серверу. А сам вычисляет ключ возводя вычисленное число от сервера в степень своей закрытого ключа б и находит остаток от деления на п.

Тож самое делает С: возводит в степень своего закрытого ключа а вычисленное число от клиента число Б и находит остатот от деления на п.

Т.о.получаются одинаковые ключи с помощью которых можно шифровать сообщение. Криптостойкость обеспечивается за счет того, что генерируются большие закрытые ключи а и б, что позволяет делать долгий перебор.

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

ЦП – преобразование над каким-то блоком данных. Его будем передавать вместе с этими данными для того, чтобы проверить что эти данные не были изменены и владелец остался тем же.