Лабораторная работа 27

ПСКП

ПОИТ-3

**Задание 01**

1. Разработайте клиент-серверное приложение **27-01**(**27-01s** – server (EXPRESS), **27-01c** – 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 **27-02**(**27-02s** – server (EXPRESS), **27-02c** – 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 цифровую подпись и выводит сообщение с результатом проверки в консоль.

**Задание 03**. Ответьте на вопросы

1. Что такое хеш-функция?
2. Что такое хеширование?
3. Перечислите известные алгоритмы хеширования.
4. Поясните понятие «сеансовый ключ».
5. Поясните понятия «публичный» и «приватный» 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.