БРАУЗЕР НЕ НАДО, ТОЛЬКО В КОНСОЛИ ЗАПУСТИТЬ С И К

1) К: делает запрос на получение контекста для генерации симм. ключа для шифрования

С: получает запрос от клиента  
 формир серверный контекст для отправки (serverDH.**getContext**())  
 отправляет серверный контекст

К: получает серверный контекст (**ClientDH**(ServerContext))  
 вычисляет ключ для шифрования (clientDH.**getSecret**(serverContext))  
 формир клиентский контекст для отправки (clientDH.**getContext**())  
 отправляет клиент. контекст

С: получ клиентский контекст  
 вычисляет ключ для шифрования (serverDH.**getSecret**(clientContext);

**1 ЗАДАНИЕ (23-01m.js)**

1) К делает get / (запрос на получение контекста)  
2) С формир *серв.контекст*, отправляет в json(ServerDH(1024, 3).getContext())  
3) К формир из него *клиен.контекст* (ClientDH(servContext) .getContext())  
4) К делает post /setKey   
5) С вычисляет *ключ для шифрования* (serverDH.getSecret(clientContext))  
 С выводит его key = serverSecret: …  
 С считывает файл in.txt  
 С зашифровывает его с пом. ключа cipherfile(in.txt, ch.txt, key)  
 С записывает это в ch.txt  
 С отправляет ‘Success’   
6) К делает get /resource  
7) С проверяет serverSecret, определен ли  
 С откр ch.txt для чтения  
 С записывает его содержимое в **res**  
 С выводит это в консоль  
8) К вычисл ключ для шифрования (clientDH.getSecret(servContext)  
 К записывает этот ключ в key  
 К дешифрует ответ сервера с пом. ключа и запис это в de.txt decipher(res,file,key)  
 К выводит parms

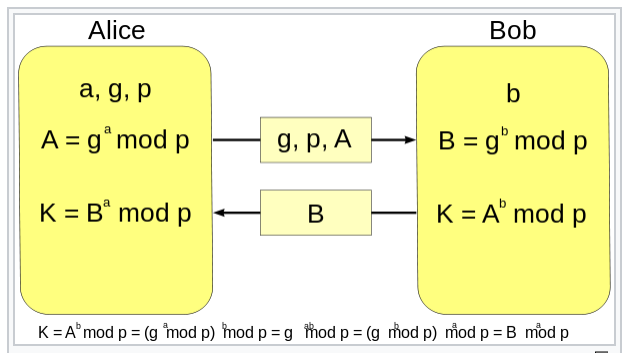
нарушение схемы обмена д-ми == 409

23-01m.js

**cipher:** AES: преобр блок [128] в другой с пом. ключа  
piv – пустой буфер 16 октетов [128]  
pk – ключ, не задан – рандомный [32]  
ch – объект Cipher, кот. исп заданные alg, key и вектор инициализации iv

**decipher:**   
alg – aes-256-cbc  
piv – пустой буффер 16 октетов [128]  
dch – объект Decipher, исп. flg, key, вектор инициализации iv

23-01m2.js



класс DiffieHellman – для создания обмена ключами Диффи-Хеллмана  
 getPrime – простое число ДХ  
 getGenerator – генератор ДХ   
 generateKeys – генер приват и откр ключи ДХ и возвр откр. ключ  
getContext – получ 8-ричное представление всего  
getSecret – с пом computeSecret вычил разделенный секрет, исп-я откр.ключ

2 задание

С отправл txt-файл (ФИО в откр виде) + цифр.подпись  
К провер цифр.подпись и выводит результат проверки

1) К делает GET /resource  
2) С считывает in.txt  
 С записывает это в res  
3) К открывает out2.txt для записи  
 К записывает туда res от сервера  
 К делает GET /  
4) С создает ЭЦП ss =ServerSign ()  
 С откр in.txt для чтения  
 С отправляет контекст подписи ss.getSignContext(rs)  
5) К создает ClientVerify (контекст подписи)  
 К считывает out2.txt  
 К вызыв. метод verify (rs) класса ClientVerify – провер ЭЦП  
 К выводит результаты

1. 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

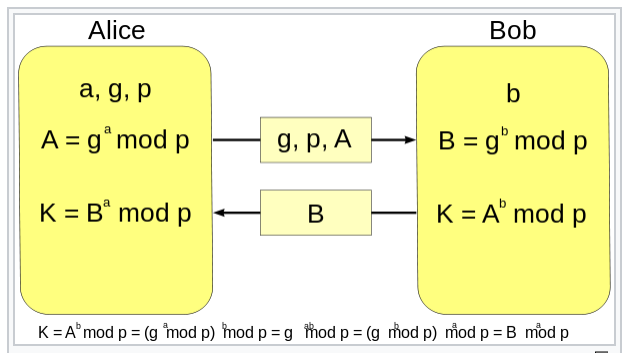
1. Поясните понятие «дайджест»

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