

## Домашнее задание 4.

### Хеширование, кодирование, шифрование.

### Протокол HTTPS

Во всех заданиях, в которых необходима работа с консольными клиентами, в ответах необходимо указывать команду, которую Вы выполняли, и ее результат. Так же дать ответы на вопросы задания.

#### ХЕШИРОВАНИЕ

1. Используя консольные утилиты хеширования по алгоритмам *MD5* и *SHA* посчитайте хеши для Вашего адреса email. Для *SHA* используйте несколько возможных в утилите вариантов алгоритма подсчета хеша.
2. Для установки ОС Linux Вы скачивали образ дистрибутива, для каждого образа производителя предоставляется хеш-сумма образа для проверки целостности загруженного файла. Сравните хеши загруженного Вами образа с предоставленными поставщиком.

#### КОДИРОВАНИЕ

3. Закодируйте и затем декодируйте Ваши имя и фамилию алгоритмами *BASE64* и *UUENCODE*.

#### ШИФРОВАНИЕ

4. Обратитесь браузером к адресам <https://i-ts.sirius-systems.ru> и <https://i-ts-s.sirius-systems.ru>. Чем отличается результат обращения к сайтам и почему? Установилось ли защищенное соединение с хостами?
5. Обратитесь консольным клиентом к адресу <https://i-ts.sirius-systems.ru>. Удалось ли установить защищенное соединение? Найдите в расширенном выводе консольного клиента информацию о процессе установки шифрованного соединения, опишите каждый шаг: что на нем происходит и кто является инициатором шага - клиент или сервер.
6. Обратитесь консольным клиентом к адресу <https://i-ts-s.sirius-systems.ru>. Удалось ли установить защищенное соединение? Найдите в расширенном выводе консольного клиента информацию о расположении файла с информацией о доверенных центрах сертификации. Найдите аргумент консольного клиента, позволяющий установить защищенное соединение, если это не удалось сделать сразу для адреса <https://i-ts-s.sirius-systems.ru>.
7. При помощи консольной утилиты *time* замеряйте время на обращение методами *GET* и *HEAD* к адресам <https://i-ts.sirius-systems.ru> и <http://i-ts.sirius-systems.ru>. Почему времена отличаются при использовании разных методов и разных адресов? Подсчитайте примерное время на получение тела ответа (порядок времени) и примерное время на установку защищенного соединения.