Курсовой проект.

Аутентификация с асимметричными алгоритмами шифрования в сети Интернет

Порядок выполнения лабораторной работы:

1. Выбрать не менее 3-ёх web-серверов сети Интернет различной организационной и государственной принадлежности.
2. Запустить Wireshark/tcpdump в режиме записи.
3. Используя Firefox/Chrome/Safari/ИнойБраузер установить https соединение с выбранным сервером и убедиться в установке соединения.
4. Сохранить данные необходимы для последующего сравнительного анализа:

* Имя сервера, его характеристики.
* Версия TLS.
* Выбранные алгоритмы шифрования.
* Полученный сертификат: версия, действителен ли сертификат, правильность ключа, удостоверяющий центр.
* Время установки соединения (от ClientHello до Finished)

5. Если список исследуемых серверов не исчерпан выбрать другой сервер и повторить соединение.
6. Если браузер поддерживал соединение TLS 1.2 / 1.3 принудительно изменить параметры TLS
(для соединения в Firefox на TLS 1.0 / 1.1 в браузере перейти по адресу “about:config” и изменить раздел SSL\TLS, security.tls.version.enable-deprecated) и провести попытки соединения с выбранными серверами.
7. Провести сравнительный анализ полученной информации.
8. В качестве отчета представить результаты сравнительного анализа, выводы в отношении безопасности и корректности настройки веб-серверов с учетом их организационной и государственной принадлежности.