Лабораторная №4.

Аутентификация с асимметричными алгоритмами шифрования

Порядок выполнения лабораторной работы:

1. Выбрать не менее 2-ух web-серверов сети Интернет различной организационной и государственной принадлежности.
2. Запустить Wireshark и используя Firefox установить https соединение с выбранным сервером.
3. Провести анализ соединения.
4. Сохранить данные необходимы для последующего сравнительного анализа:

Имя сервера, его характеристики.

Версия TLS.

Выбранные алгоритмы шифрования.

Полученный сертификат: версия. Валидность сертификата, валидность 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 принудительно изменить параметры TLS соединения в Firefox на TLS 1.0 (в браузере перейти по адресу “about:config” и изменить раздел SSL\TLS) 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.