Лабораторная №6

Аутентификация

Цель работы:

Получить представление о механизмах аутентификации.

Задача.

Разработать веб-приложение с формой для аутентификации. Аутентификацию осуществлять при помощи протокола SRP [1, 2] или при помощи OPAQUE [3, 4, 5]. Можно (и нужно) использовать существующие реализации/библиотеки.

1. https://ru.wikipedia.org/wiki/SRP
2. https://habr.com/ru/post/121021/
3. https://eprint.iacr.org/2018/163.pdf
4. https://blog.cryptographyengineering.com/2018/10/19/lets-talk-about-pake/
5. https://github.com/stef/libsphinx