Лабораторная работа №2

Карпов Алексей

12 группа кафедра ИСУ

Вариант 3

**AES**

Данный алгоритм преобразует один 128-битный блок в другой, используя секретный ключ который нужен для такого преобразования. Для расшифровки полученного 128-битного блока используют второе преобразование с тем же секретным ключом.

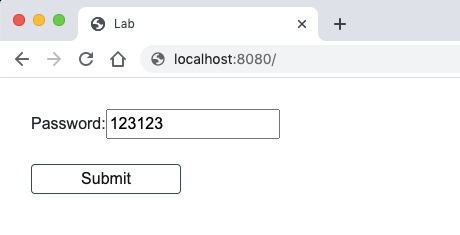
Размер блока всегда равен 128 бит. Размер ключа также имеет фиксированный размер. Чтобы зашифровать произвольный текст любым паролем, можно поступить так:

1. Получить хеш от пароля
2. Преобразовать хеш в ключ по правилам описанным в стандарте AES
3. Разбить текст на блоки по 128 бит
4. Зашифровать каждый блок функцией cipher

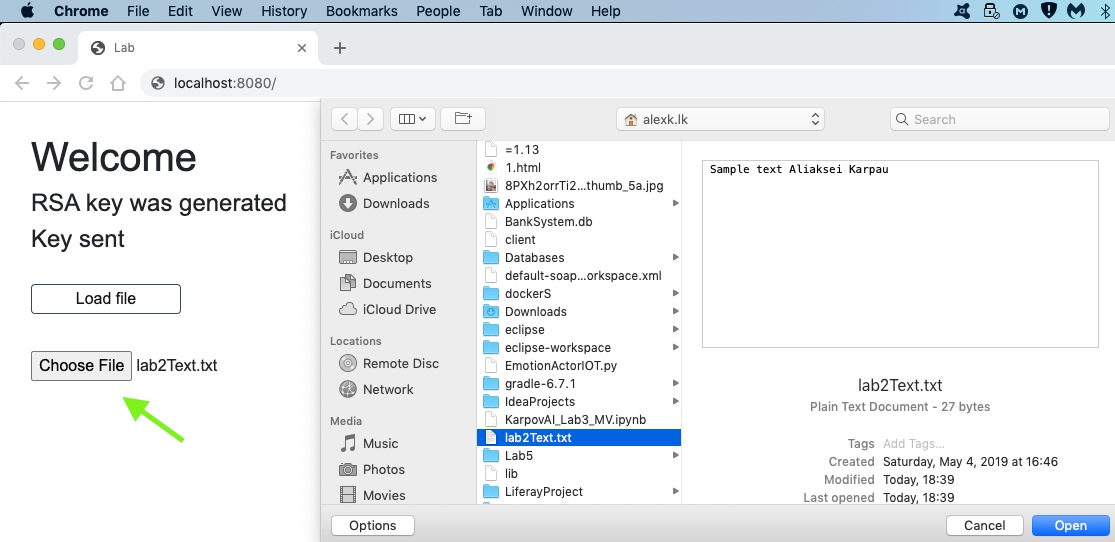
**Задание**

**Клиент:**

Генерация ключа и отправка

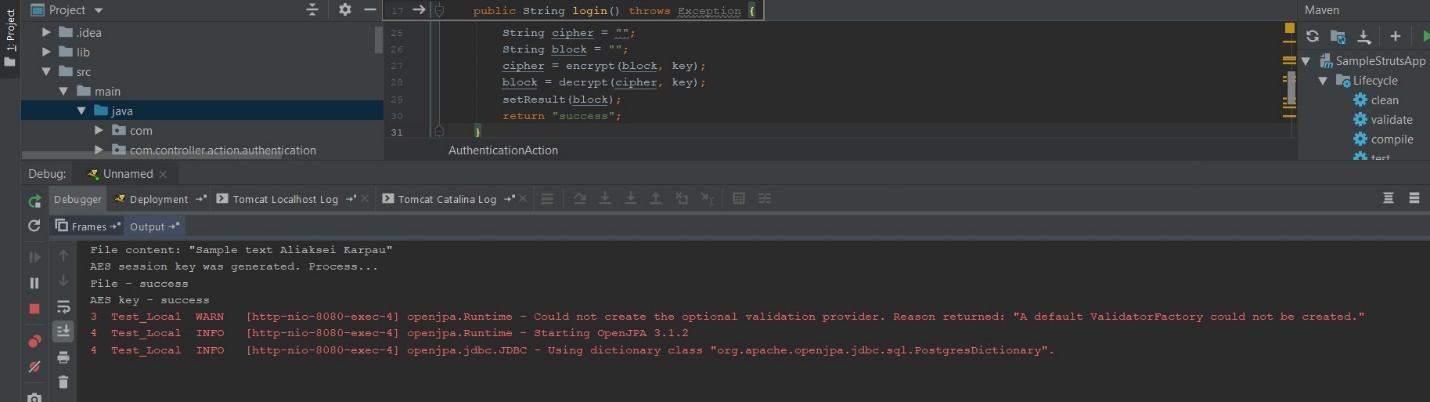


Выбор файла для шифровки и запрос на генерацию сеансового ключа:



**Сервер:**

Шифровка, выбранного файла идёт c помощью сеансового ключа, затем сеансовый ключ также шифруется уже открытым ключом и отправляется клиенту.



**Клиент:**

Результат работы клиента по расшифровке:

