Лабораторная работа №2

Дворяков Максим

12 группа кафедра ИСУ

Вариант 3

В результате проведения лабораторной работы были достигнуты следующие результаты:

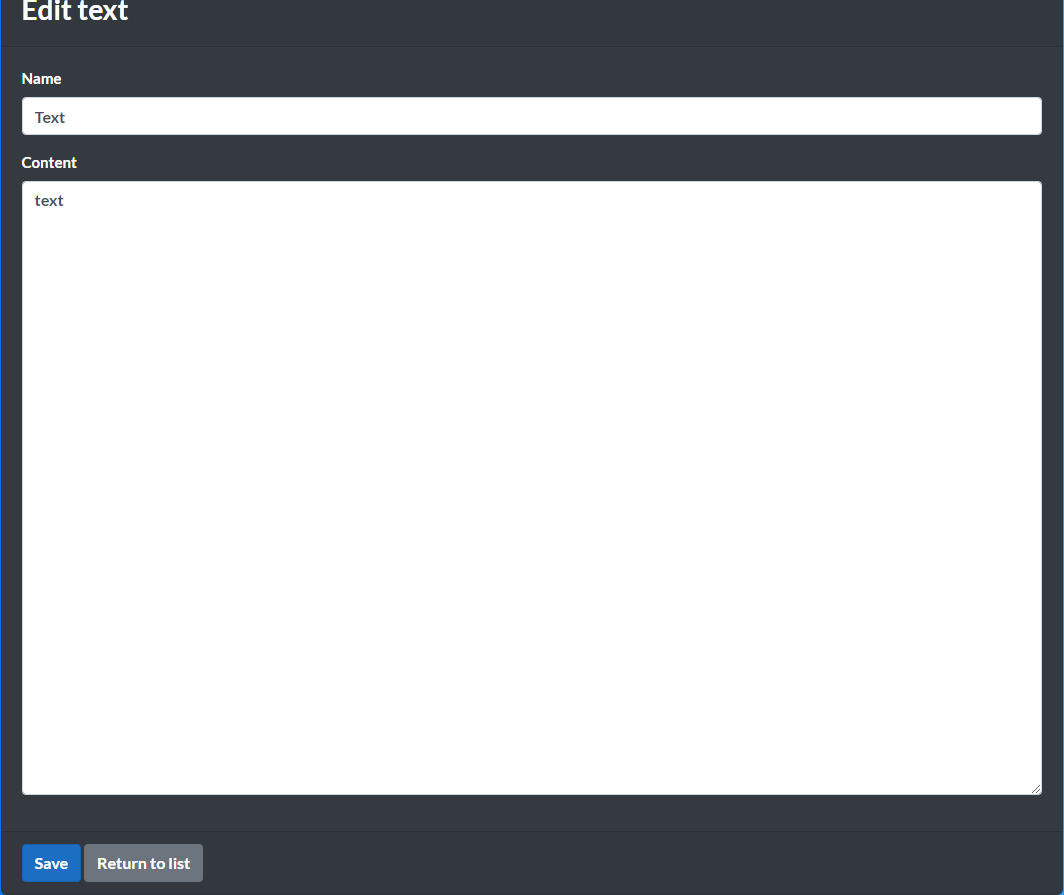
1. Было разработано клиент-серверное приложение, которое отвечает требованиям, перечисленным в условии.

2. Изучены алгоритмы шифрования .

Показываю пример работы программы по каждому из пунктов.

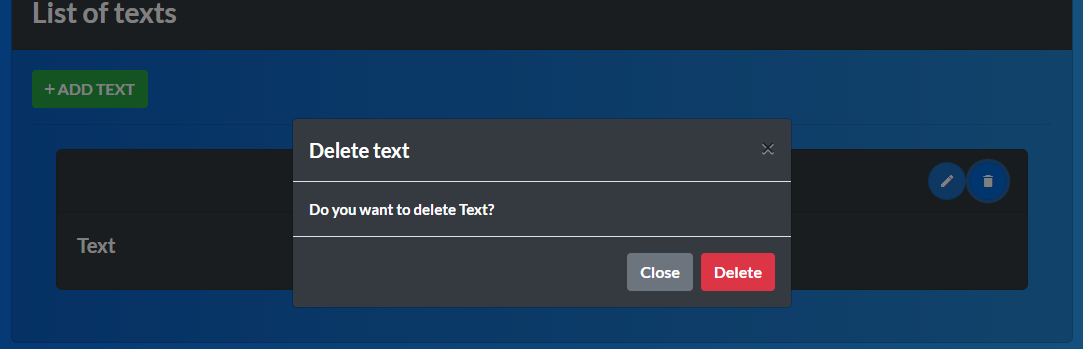
Для примера возьмём метод Edit. В данном случае будет использоваться 128-битный ключ и 128-битный IV. Размер ключа в RSA будет равен 2048-битам.

Для начала на сервере шифруется текст сеансовым ключом, AES преобразует один 128-битный блок в другой, используя секретный ключ который нужен для такого преобразования. После чего данный текст отправляется клиенту, вместе с сеансовым ключом, зашифрованным при помощи RSA. По приходу на клиент, происходит расшифровка сеансового ключа, после чего, происходит расшифровка зашифрованного текста. Для расшифровки полученного 128-битного блока используют второе преобразование с тем же секретным ключом.

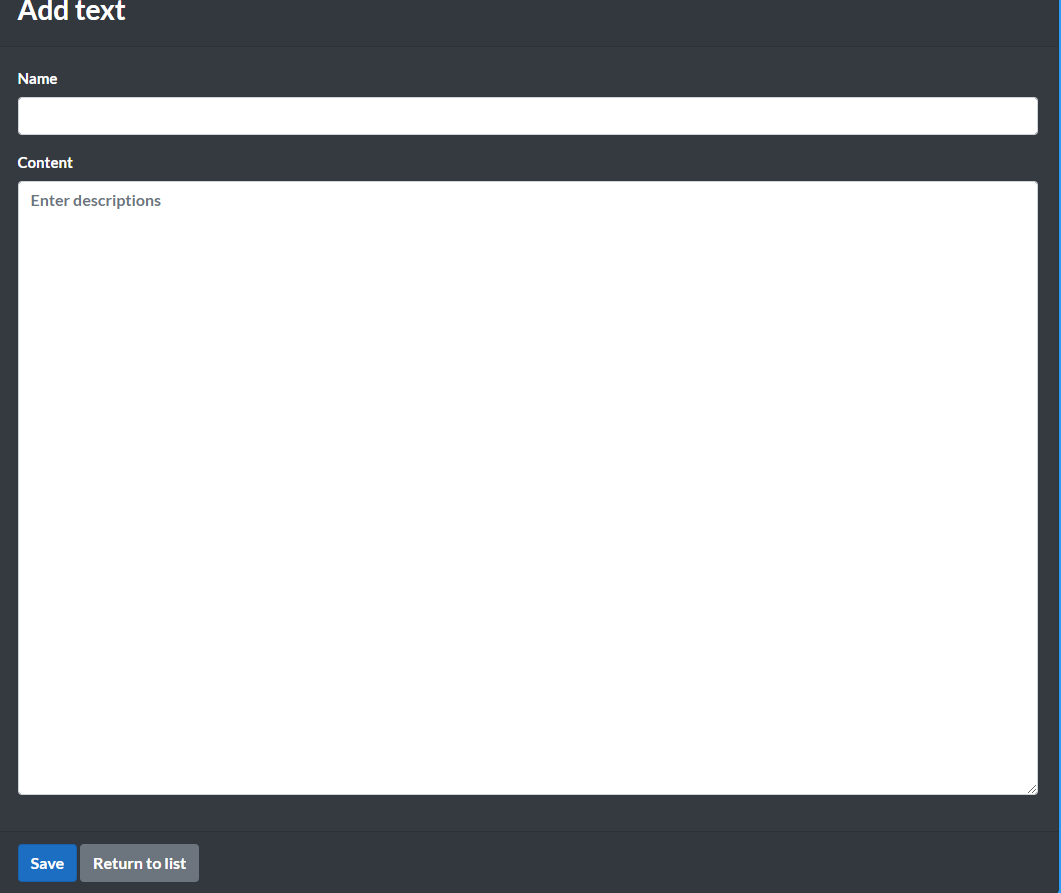


После чего делаем какие-то изменения, текст повторно шифруется сеансовым ключом и отправляется на сервер, где по прибытию происходит дешифровка и сохранение текста в базу данных.

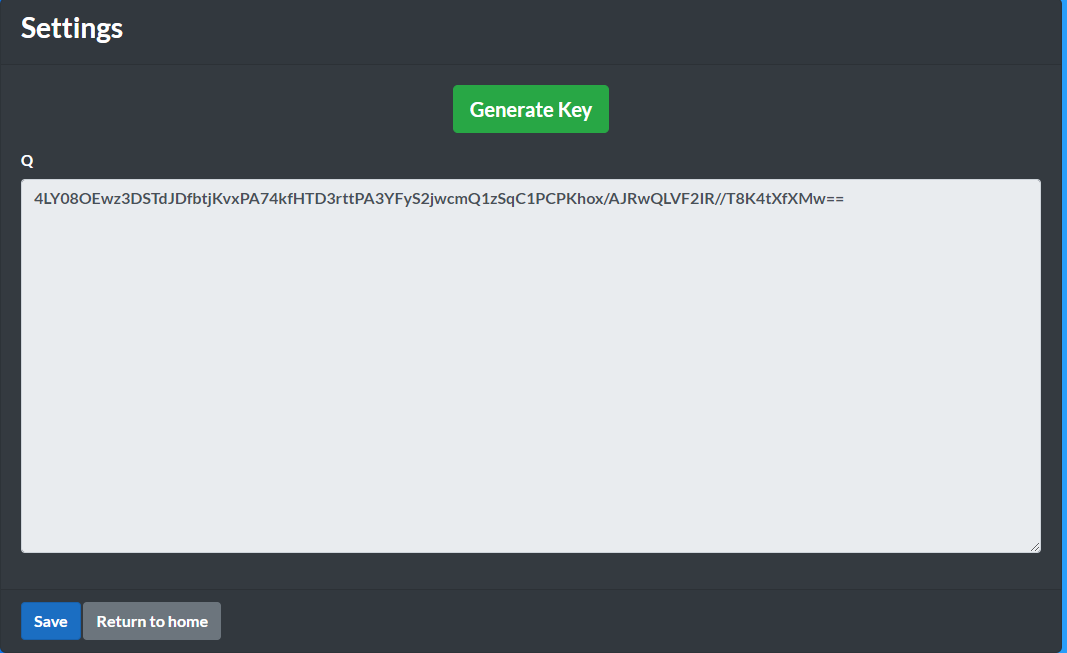
Так же есть возможность удалить текст.



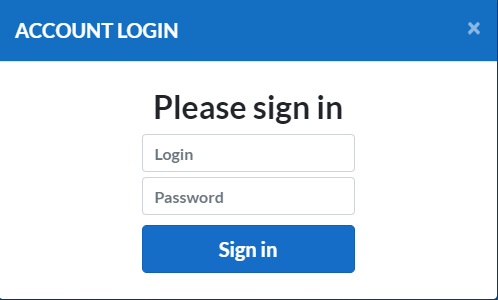
Ещё есть возможность добавить новый текст



Так же реализована возможность создавать новый закрытый ключ



На дополнительный баллы была организована аутентификация



А так же веб сайт можно открыть на мобильном устройстве.

