**Отчет по лабораторным работам №2 и №4**

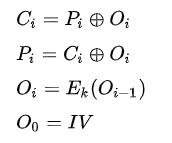
**“Защищенный блокнот”**

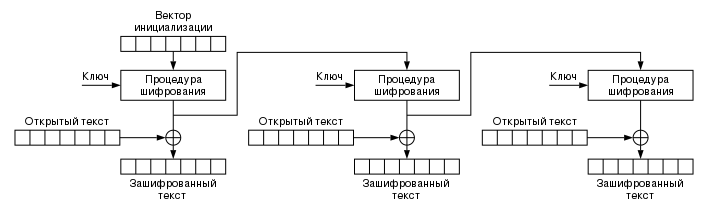
**Вариант 3:** AES, режим обратной связи по выходу (OFB – Output Feed Back).

Advanced Encryption Standard (AES), также известный как Rijndael — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES.

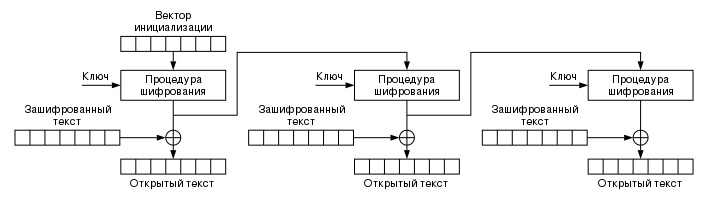
Режим обратной связи по выходу (OFB) превращает блочный шифр в синхронный шифр потока: он генерирует ключевые блоки, которые являются результатом сложения с блоками открытого текста, чтобы получить зашифрованный текст. Так же, как с другими шифрами потока, зеркальное отражение в зашифрованном тексте производит зеркально отражённый бит в открытом тексте в том же самом местоположении. Это свойство позволяет многим кодам с исправлением ошибок функционировать как обычно, даже когда исправление ошибок применено перед кодированием.

Из-за симметрии операции сложения, шифрование и расшифрование похожи:





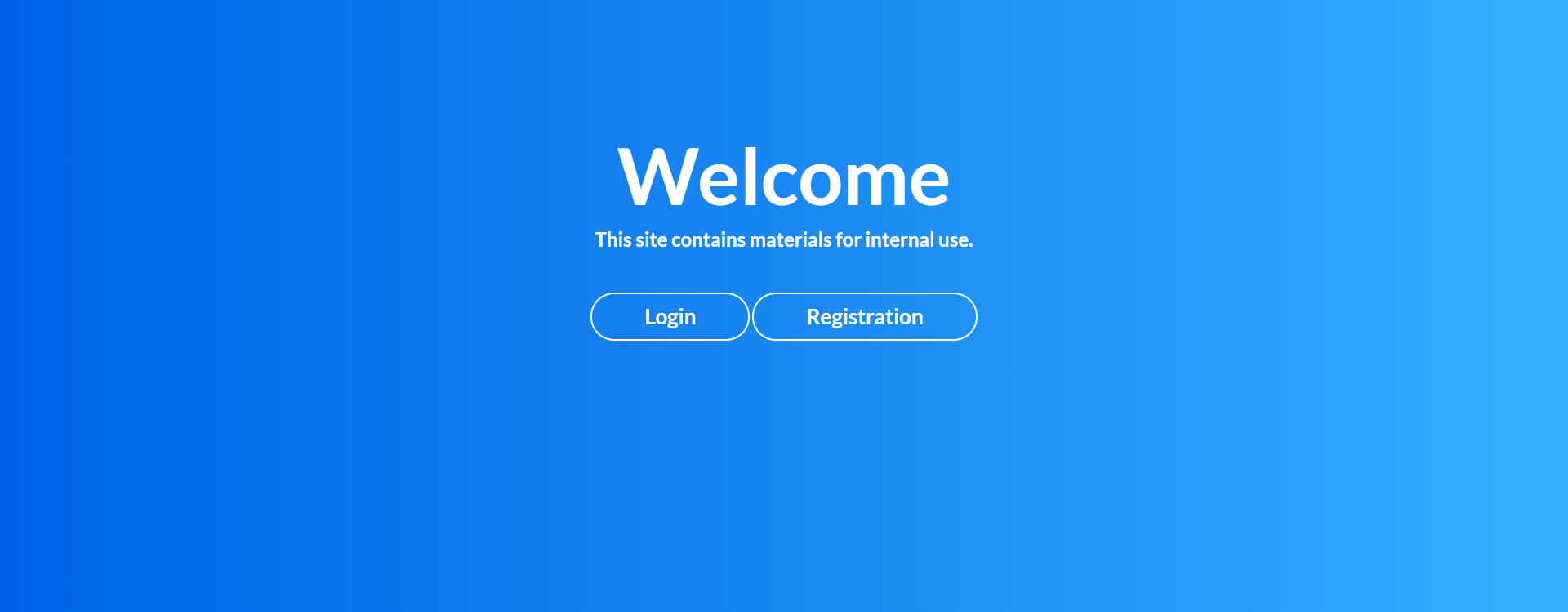
Шифрование в режиме OFB

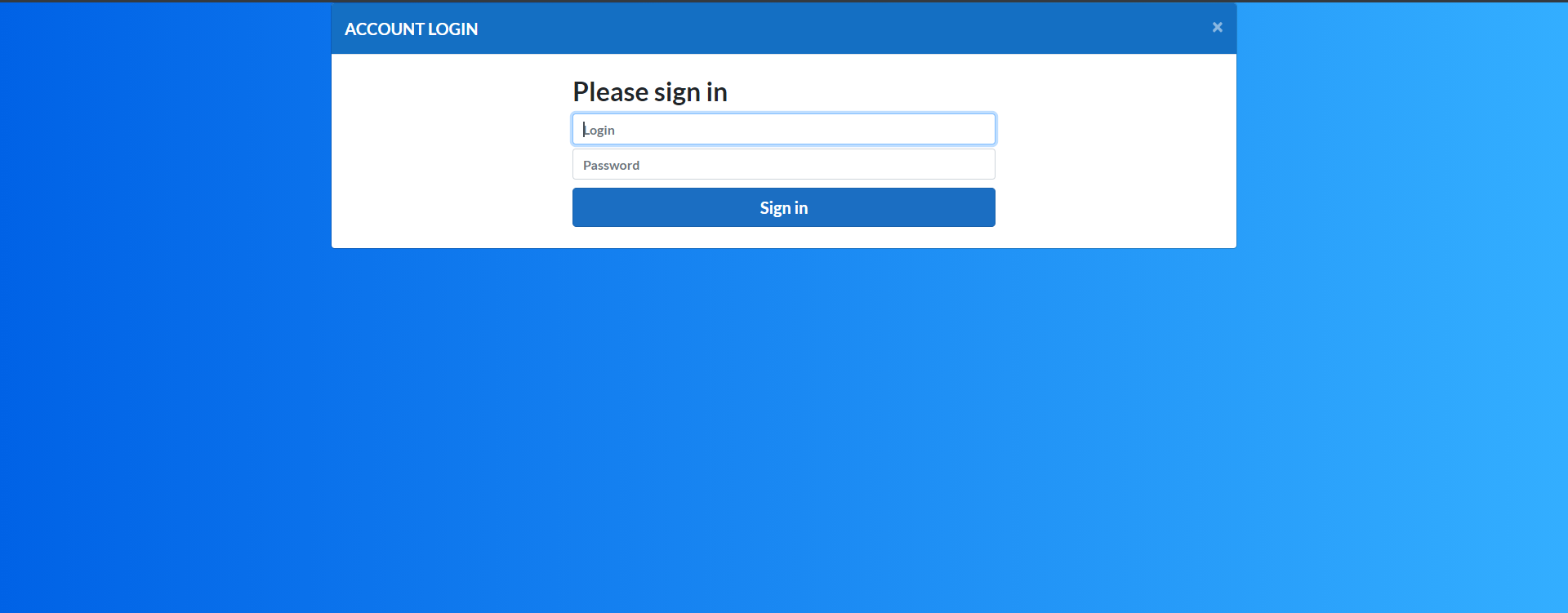


Расшифровка в режиме OFB

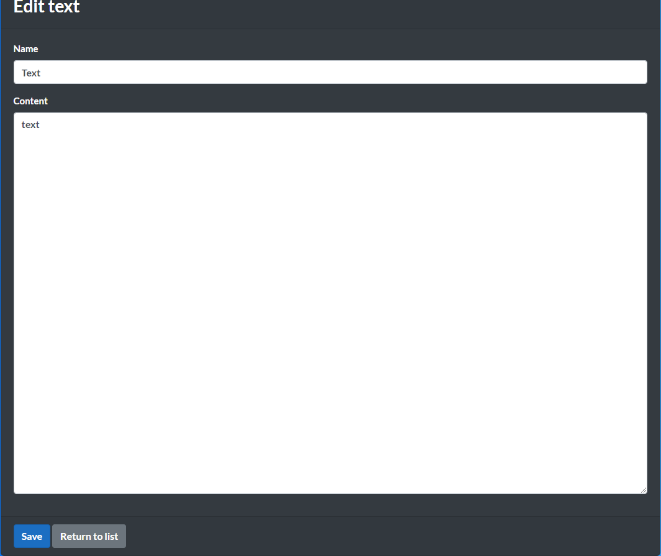
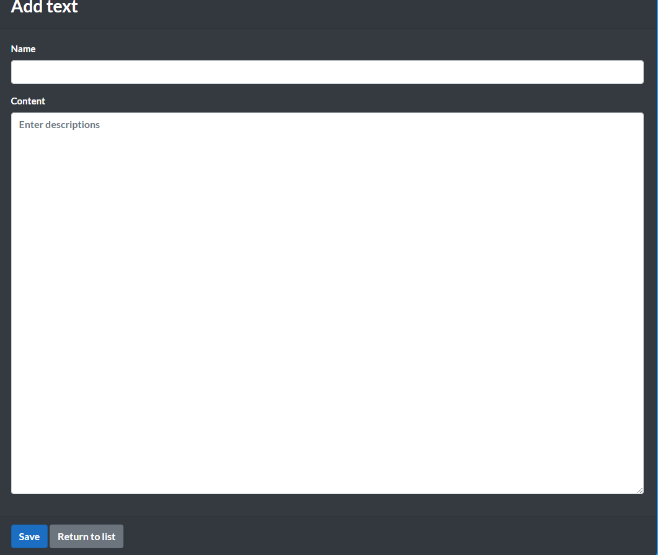
**Реализация**

В приложении реализована аутентификация

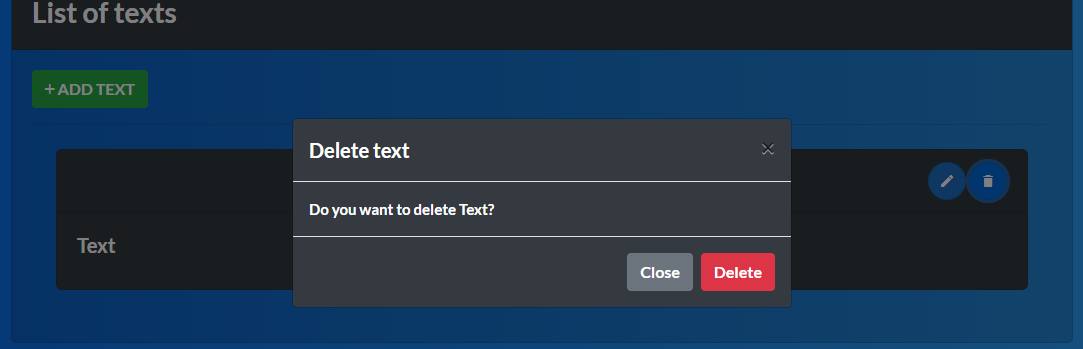




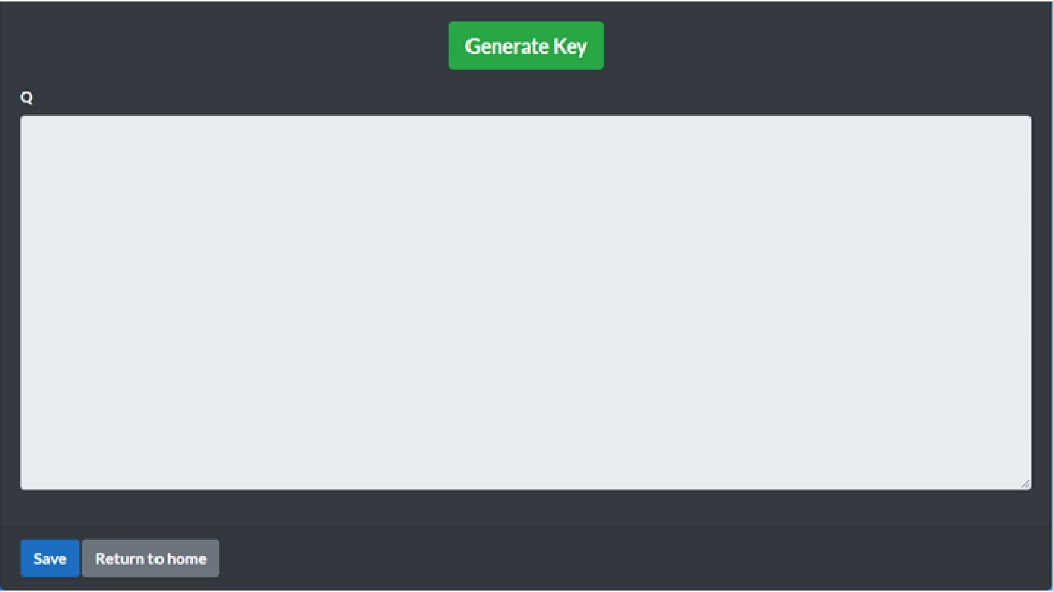
Добавление текста в блокнот:



Удаление текста из блокнота:



А также его редактирование. Генерация нового закрытого ключа RSA:



Длина ключа RSA: 2048 бит

Длина блока AES: 128 бит

RSA используется для шифрования и расшифровки сеансового ключа.

**2 лабораторная работа:**

Открытый ключ RSA один раз отправляется клиентом серверу. После запроса (на изменение) текстового файла – нажатия на имя в списке личных файлов – клиент отправляет запрос на сервер с именем выбранного файла. Сервер генерирует случайный сеансовый ключ, шифрует текст этим сеансовым ключом текстовый файл (блоки проходят преобразование в соответствии с раундами алгоритма AES на основании секретного ключа в режиме OFB), а сам сеансовый ключ шифрует открытым RSA ключом и отправляет все перечисленное клиенту. При получении этих данных, клиент расшифровывает сеансовый ключ закрытым RSA ключом, а затем текст полученным сеансовым ключом (при этом блоки проходят преобразование, обратное тому, что совершалось при шифровании на сервере, с идентичным ключом). Если на клиенте текст изменяется и отправляется запрос на сохранение, производится процедура шифрования текста сеансовым ключом, полученным от сервера, оправка этого шифртекста на сервер, где происходит расшифровка и сохранение в базу данных. Для хранения данных пользователей и их текстовых документов использовался MS SQL Server.

**4 лабораторная работа:**

Помимо AES текстовый файл также сначала шифруется заданным паролем пользователя.

**Возможные атаки**

«Защищенный блокнот» не может быть подвержен атаке на функционал восстановления паролей или обходу CAPTCHA, т.к. не реализует данный функционал.

Многоразовое хеширование пароля для аутентификации обеспечивает безопасность в случае атак на пароли, слабый и универсальный пароль.