Практическая работа №5
Тема: End-to-End (E2E) шифрование

Цель работы
Познакомиться с процессом End-to-End (E2E) шифрования на примере реализации простого мессенджера.

Технические требования
• Наличие Docker и Docker Compose
• Наличие cURL / Postman / Insomnia
• Редактор кода (например, Visual Studio Code)
• Node.js и библиотека CryptoJS

Теоретическая часть
End-to-End (E2E) шифрование — это метод защиты данных, при котором сообщение шифруется на устройстве отправителя и расшифровывается только на устройстве получателя. Сервер выступает лишь посредником, не имея возможности прочитать содержимое сообщений.

Практическая часть
В ходе выполнения работы был создан простой чат-сервер на Node.js с использованием WebSocket (socket.io). Клиентская часть была модифицирована с применением библиотеки CryptoJS для шифрования и расшифровки сообщений.

Фрагмент кода клиентской части (index.html)

```
<script src="https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.2.0/crypto-
js.min.js"></script>
<script src="/socket.io/socket.io.js"></script>
<script>
  const socket = io();
  socket.on('new message', (encryptedMsg) => {
    const key = document.getElementById('key').value;
    const bytes  = CryptoJS.AES.decrypt(encryptedMsg, key);
```

```
    const originalText = bytes.toString(CryptoJS.enc.Utf8);
    const li = document.createElement('li');
    li.textContent = originalText || "[Ошибка дешифрования]";
    document.getElementById('chat').appendChild(li);
  });

  function sendMessage() {
    const msg = document.getElementById('message').value;
    const key = document.getElementById('key').value;
    const encrypted = CryptoJS.AES.encrypt(msg, key).toString();
    socket.emit('new message', encrypted);
  }
</script>
```

Результаты работы

После реализации шифрования сервер начал получать зашифрованные строки вида:

📨 Получено сообщение:
U2FsdGVkX19qbMh9XeQlE2Z+4Ije2/3JoYuXntjgDRQ=

На клиентской стороне сообщение успешно расшифровывается при совпадении ключа.

Интерфейс чата

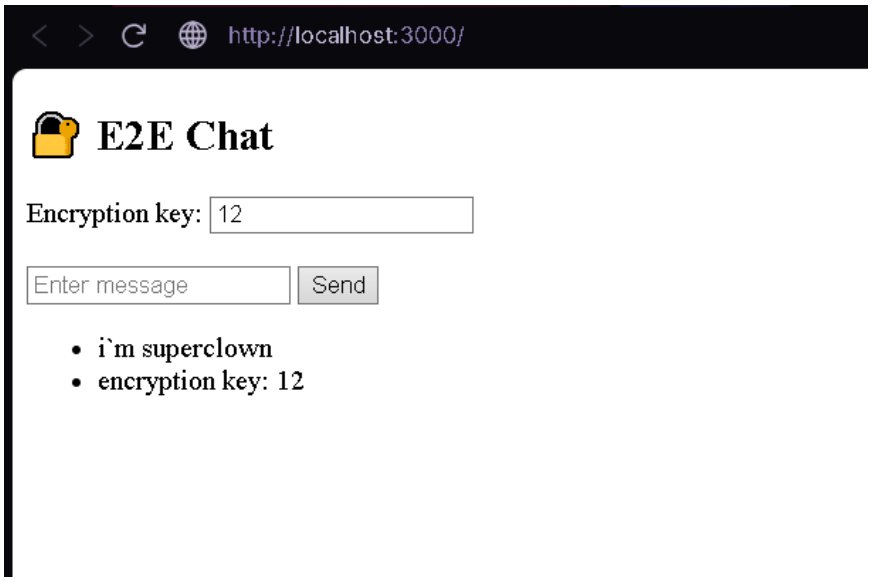

Рис. 1. Интерфейс чата с E2E шифрованием.

Заключение

В ходе практической работы был реализован механизм end-to-end шифрования для передачи сообщений в чате. Сообщения шифруются на стороне клиента и передаются на сервер в зашифрованном виде. Сервер не имеет доступа к содержимому сообщений, что обеспечивает высокий уровень конфиденциальности.