Escuela Superior
de Ingeniería y Tecnología
Universidad de La Laguna

Grado en Ingeniería Informática
Curso 2024-2025

PROYECTO DE TRABAJO DE FIN DE GRADO

Apellidos y nombre del alumno: LORENZO SÁNCHEZ, SAMUEL
DNI: 42419435Y

Apellidos y nombre del tutor: CABALLERO GIL, PINO
DNI: 45534310Z

Apellidos y nombre del cotutor: PERÉZ RAMOS EDGAR
DNI: 42199515N

Título del Proyecto: "Creación de un chat seguro con CRYSTALS".

1. Introducción

(Máximo 1 página)

La criptografía ha recorrido un largo camino desde sus inicios en la antigüedad. Comenzó con métodos como la Escítala en el siglo V a.C., un sistema de trasposición que utilizaba un cilindro para cifrar y descifrar mensajes, y el Cifrado César. Posteriormente, en el Renacimiento, figuras como Leon Battista Alberti y Blaise de Vigenère hicieron avances significativos con la introducción de sistemas de sustitución polialfabética. Durante los siglos XVII y XVIII, la criptografía se utilizó en contextos militares y políticos, con episodios notables como el criptoanálisis que llevó a la ejecución de María Estuardo.

En el siglo XX, la criptografía experimentó un gran desarrollo teórico y práctico, especialmente durante las dos guerras mundiales. La máquina Enigma y la máquina Lorenz, utilizadas por los alemanes durante la Segunda Guerra Mundial, son ejemplos destacados de la complejidad alcanzada. Tras la guerra, la teoría de la información de Claude Shannon y el desarrollo del Estándar de Cifrado de Datos (DES) en los años 70 marcaron hitos importantes. Finalmente, la introducción de la criptografía asimétrica revolucionó el campo, permitiendo aplicaciones modernas como la firma digital y mejorando significativamente la seguridad de las comunicaciones.

La criptografía tiene la misión de proteger la información de agentes no deseados, lo cual se logra mediante el uso de algoritmos, hashes y firmas. La información puede estar almacenada en un servidor, en movimiento al intercambiarse entre varios ordenadores, o en uso mientras se ejecutan operaciones de computación en los datos.

En la actualidad, la criptografía está en jaque debido a la aparición de los ordenadores cuánticos, que pretenden revolucionar lo que conocemos por ciberseguridad en todo tipo de ámbitos como la medicina, la física y el ámbito militar. Es por este motivo que este Trabajo de Fin de Grado busca poner en práctica y llevar a cabo la integración del algoritmo de cifrado post-cuántico CRYSTALS-Kyber y el algoritmo de firma CRYSTALS-Dilithium en una aplicación de mensajería instantánea llamada Crypto Chat, la cual busca sentar las bases de la computación cuántica.

Es relevante desarrollar una aplicación que integre el algoritmo post-cuántico porque gran parte de las aplicaciones actuales no están preparadas para ataques con ordenadores cuánticos. Aunque estos ataques aún se ven lejanos debido a que los ordenadores cuánticos continúan en desarrollo, tarde o temprano tendremos que emigrar a estos sistemas si no queremos que nuestros datos puedan ser vulnerados por agentes externos.

2. Antecedentes y estado actual del tema

(Máximo 1 página)

La criptografía ha evolucionado desde simples técnicas usadas en la antigüedad, hasta complejos sistemas digitales actuales. Sus inicios se remontan al antiguo Egipto donde se empleaban métodos de cifrado rudimentarios como el cifrado Cesár, el cual desplazaba las letras de un mensaje de acuerdo con una clave fija. Durante la edad media Al-Kindi, consiguió romper los cifrados por sustitución.

A partir del Renacimiento, aumento la complejidad de la criptografía, especialmente en Europa, debido a conflictos políticos y religiosos. Sin embargo, los métodos criptográficos seguían siendo vulnerables a ataques avanzados. En este período, se desarrolló la máquina Enigma, marcó un hito en el progreso de esta disciplina.

Durante la Segunda Guerra Mundial, la criptografía jugó un papel crucial, la máquina Enigma, fue rota por matemáticos polacos y británicos, como Marian Rejewski y Alan Turing.

Con la llega de la era moderna, Claude Shannon revoluciono el campo al establecer una basé teórica para la criptografía con su teoría de la información. En los años 70, la criptografía dejo ser exclusiva del gobierno, gracias a la invención de la criptografía asimétrica y la creación de estándares públicos como el DES, marcando el inicio de la criptografía común y el establecimiento de la seguridad en las comunicaciones digitales. Además, aparece la criptografía de clave pública por Whitfield Diffie y Martin Hellman.

Sin embargo, la llegado de la criptografía cuántica, propuesta inicialmente por Stephen Wiesner marca un nuevo capítulo en esta evolución. Este sistema utiliza los principios de la mecánica cuántica para garantizar la confidencialidad de la información transmitida. Una de las propiedades más importantes de la criptografía cuántica es que si un tercero intenta espiar durante la creación de la clave secreta, el proceso se altera detectándolo al intruso antes de que se transmita la información

3. Actividades a realizar

(Máximo 1 página)

Se realizarán las siguientes actividades:

1. **Configurar el entorno de desarrollo y estructura del proyecto**: Crear el repositorio de código, configurar dependencias principales y el entorno de trabajo con Node.js y MongoDB Atlas.
2. **Diseñar y modelar la base de datos en MongoDB**: Crear los esquemas de usuarios, mensajes y conversaciones, asegurando que se ajusten a los requisitos de la aplicación.
3. **Desarrollar el sistema de autenticación y autorización con JWT**: Implementar flujos de registro, inicio de sesión y cierre de sesión usando JSON Web Tokens.
4. **Implementar cifrado post-cuántico CRYSTALS-Kyber para la mensajería**: Configurar y aplicar CRYSTALS-Kyber en el backend para cifrar los mensajes enviados entre usuarios.
5. **Integrar firma digital CRYSTALS-Dilithium para autenticación de mensajes**: Incorporar el esquema de firma Crystal Dilithium para firmar y verificar la autenticidad de los mensajes
6. **Desarrollar la funcionalidad de chat en tiempo real usando Socket.io**: Configurar Socket.io en el servidor y el cliente para que los mensajes se transmitan en tiempo real.
7. **Diseñar y desarrollar la interfaz de usuario (UI) en Figma y React**: Crear el diseño visual de la interfaz en Figma y desarrollar componentes en React para registro, login, lista de conversaciones, y chat.
8. **Incorporar funcionalidades de búsqueda, eliminación de mensajes antiguos y envío de archivos**: Implementar una búsqueda de usuarios y añadir la función de eliminar mensajes después de 7 días.
9. **Implementar autenticación facial y verificación de cifrado extremo a extremo mediante código QR**: Configurar autenticación facial para añadir una capa de seguridad avanzada en el inicio de sesión. Ademas de, implementar una función que genere un código QR para verificar el cifrado extremo a extremo de las conversaciones.
10. **Desplegar la aplicación en la nube y realizar pruebas finales**: Configurar el entorno de producción y desplegar la aplicación en Render

4. Plan de Trabajo

(Máximo 1 página)

Mes 1: Configuración e Implementación del Backend Básico

- **Semana 1:** Configuración del entorno de desarrollo (repositorio, dependencias, MongoDB Atlas). Definir la estructura de la base de datos (usuarios, mensajes, conversaciones).Crear la arquitectura base del backend y del frontend.
- **Semana 2:** Implementación del sistema de autenticación (registro, inicio/cierre de sesión) con JWT. Configuración de cookies seguras y middleware para proteger rutas.
- **Semana 3:** Integración de cifrado post-cuántico con CRYSTALS-Kyber para asegurar mensajes.
- **Semana 4:** Incorporación de CRYSTALS-Dilithium para firmas digitales en los mensajes. Validaciones de firma para asegurar la integridad de los mensajes.

Mes 2: Desarrollo del Backend Avanzado e Interfaz de Usuario

- **Semana 5:** Configurar mensajería en tiempo real con Socket.io (conexión y sincronización de mensajes). Pruebas de sincronización de mensajes en tiempo real entre usuarios.
- **Semana 6:** Diseño de la interfaz gráfica en Figma (pantallas de inicio, registro, chat). Desarrollo de componentes en React (registro, inicio de sesión, lista de conversaciones, chat).
- **Semana 7:** Implementar el sistema de autenticación en el frontend (gestión de sesiones y protección de rutas). Pruebas iniciales de autenticación en la interfaz de usuario.
- **Semana 8:** Incorporación de búsqueda de usuarios y eliminación automática de mensajes tras 7 días. Implementación de envío seguro de archivos (PDF e imágenes) con validación de tipo.

Mes 3: Funcionalidades Avanzadas, Integración y Despliegue

- **Semana 9:** Configurar autenticación facial para el inicio de sesión. Implementar verificación de cifrado extremo a extremo mediante código QR.
- **Semana 10:** Integrar todas las funcionalidades en la interfaz gráfica (búsqueda de usuarios, gestión de mensajes, adjuntos). Realizar pruebas de integración y resolver problemas de sincronización y rendimiento.
- **Semana 11:** Realizar pruebas de seguridad y validación de URL en mensajes.
- **Semana 12:** Despliegue en la nube (Render u otra plataforma). Pruebas finales y ajustes en entorno de producción. Documentación y preparación de la memoria del TFG.

5. Propuesta de evaluación

(Máximo 1 página)

Hito	Calificación
Configuración del entorno de desarrollo y base de datos	3
Implementación del sistema de autenticación básica (registro e inicio de sesión)	4
Integración de cifrado post-cuántico CRYSTALS-Kyber para mensajes	5
Firma digital de mensajes usando CRYSTALS-Dilithium	6
Configuración de mensajería en tiempo real con Socket.io	7
Diseño de interfaz gráfica en Figma y desarrollo básico en React	7
Desarrollo de funcionalidades adicionales: envío de archivos y búsqueda de usuarios	8
Implementación de la autenticación facial y verificación de cifrado por QR	9
Pruebas finales de seguridad, rendimiento y despliegue en la nube	9
Desarrollo de versión móvil (React Native)	10

La Laguna, 25 de Noviembre de 2024

Fdo.: