Planificación del Proyecto Criptográfico

PT Pablo Roberto García Torres

Trimestre 24-P: Fundamentos Criptográficos y Diseño de Funciones Hash

Semana 1-3: Fundamentos de Criptografía (en el documento)

- Introducción al campo de la criptografía moderna.
- Conceptos básicos de seguridad criptográfica.
- Breve historia de las funciones hash y su importancia en la criptografía.

Semana 4-6: Funciones Hash y Bibliotecas Criptográficas

- Estudio detallado de las funciones hash y sus propiedades.
- Implementación de cálculos de hash utilizando bibliotecas estándar como hashlib en Python.
- Prácticas de generación de resúmenes únicos y su aplicación en la seguridad de datos.

Semana 7-9: Tablas Hash y Almacenamiento Seguro

- Comprender la relación entre las funciones hash y las tablas hash.
- Investigación sobre trabajos previos del uso de tablas hash como funciones hash criptográficas.
- Implementación de tablas hash para almacenar y buscar resúmenes únicos.
- Ejercicios prácticos para garantizar la seguridad en el almacenamiento y búsqueda de datos.

Semana 10-11: Evaluación de Vulnerabilidades

- Investigación sobre vulnerabilidades conocidas en funciones hash.
- Análisis de técnicas de criptoanálisis para colisiones, pre-imágenes y segunda pre-imágen.
- Preparación de un informe preliminar sobre las vulnerabilidades encontradas.

Trimestre 24-O: Diseño e Implementación de Funciones Criptográficas

Semana 1-3: Generación de Claves RSA

- Estudio de RSA y su aplicación en la criptografía asimétrica (en el documento).
- Utilización de la biblioteca cryptography para generar claves RSA.
- Prácticas de firma y verificación de mensajes utilizando las claves generadas.

Semana 4-6: Algoritmos de Firmas Digitales

- Investigación sobre esquemas de firmas digitales como PKCS#1 v1.5 y ECDSA.
- Diseño y desarrollo de algoritmos de firmas digitales utilizando funciones hash y tablas hash.
- Pruebas de autenticidad e integridad de mensajes utilizando los algoritmos implementados.

Semana 7-9: Evaluación de Seguridad

- Evaluación de la seguridad y resistencia a ataques de los algoritmos implementados.
- Análisis de la eficacia de las firmas digitales en la autenticación y la integridad de datos.
- Preparación de informe intermedio sobre los resultados obtenidos.

Semana 10-11: Optimización y Mejoras

- Identificación de posibles mejoras en los algoritmos criptográficos implementados.
- Optimización del rendimiento y la seguridad de los algoritmos.
- Preparación de una presentación para discutir los avances realizados hasta el momento.

Trimestre 25-I: Conclusiones y Presentación Final

Semana 1-6: Refinamiento y Documentación

- Refinamiento de los algoritmos criptográficos basados en los resultados obtenidos.
- Documentación detallada de los algoritmos implementados y los procesos de evaluación.
- Preparación del informe a la coordinación de la Lic.

Semana 7-9: Revisión

- Revisión y corrección de posibles errores en la documentación y los algoritmos implementados.

Semana 10-11: Presentación Final y Cierre

- Presentación final del proyecto ante los asesores.
- Cierre y entrega del informe final.