INSTITUTO POLITÉCNICO NACIONAL

Escuela Superior de Cómputo

Introduction to Cryptography

Advances of project

Profesora: Sandra Díaz Santiago

Grupo: 6CM1

Integrantes:
- Rafael Alejandro Rivero Barraza
- Rojas Vazquez Diego

Fecha: 10 de Junio2024

Servicios Criptográficos Necesarios

- Confidencialidad
  La confidencialidad es esencial para proteger la privacidad y la información sensible contenida en los documentos empresariales que se subirán al sistema. Al garantizar que solo el remitente y el destinatario autorizado puedan acceder al contenido, evitamos cualquier posible exposición de datos confidenciales a terceros no autorizados, las cuales pueden resultar en pérdida de información, robo de datos o violación de la privacidad de las partes involucradas.

- Integridad
  La integridad asegura que los documentos generados no sean alterados o modificados de forma no autorizada durante su transmisión o almacenamiento. Esto es crucial para mantener la confianza en la información y evitar cualquier manipulación que pueda distorsionar el significado o la validez de los documentos. La integridad también es fundamental para cumplir con requisitos legales y regulatorios, ya que cualquier alteración no autorizada podría comprometer la validez legal de los documentos.

- Autenticación
  La autenticación verifica la identidad de los remitentes y garantiza la autenticidad de los documentos generados. Esto es crucial para evitar la suplantación de identidad y garantizar que los documentos provengan de fuentes legítimas y autorizadas. La autenticación también ayuda a establecer una cadena de confianza entre las partes involucradas en la comunicación, lo que es fundamental para construir relaciones comerciales sólidas y protegerse contra posibles fraudes o actividades maliciosas.

- Firma Digital
  La firma digital proporciona una forma segura de firmar electrónicamente los documentos, lo que garantiza su autenticidad y previene cualquier intento de repudio por parte del remitente. Además de verificar la identidad del remitente, la firma digital también garantiza la integridad del documento al proporcionar una prueba criptográfica de que el contenido no ha sido alterado desde su firma.

Algoritmos Criptográficos Propuestos

- Confidencialidad
  Se propone el uso del algoritmo de cifrado simétrico AES en modo de operación CTR. AES-CTR se eligió por ser eficiente y seguro, ya que proporciona confidencialidad al cifrar los documentos para que solo el remitente y el destinatario autorizado puedan descifrar el contenido.

- Integridad
  HMAC SHA-256 es la opción elegida para garantizar la integridad de los documentos. HMAC proporcionará una firma digital de los datos basada en la función hash SHA-256, lo que permitirá detectar cualquier modificación no autorizada en el documento durante su transmisión o almacenamiento.

- Autenticación
  RSA es un algoritmo de clave pública utilizado para la autenticación y la firma digital. La firma digital RSA proporcionará una prueba criptográfica de la autenticidad y la integridad del documento, permitiendo al destinatario verificar la identidad del remitente y garantizar que el contenido del documento no haya sido alterado. El uso de claves públicas y privadas en el esquema RSA asegura que solo el remitente autorizado pueda firmar el documento, mientras que cualquier destinatario puede verificar la firma utilizando la clave pública del remitente.

Diagrama a bloques de la arquitectura preliminar del sistema