




Laboratorio 8

Digital Signature

Juan Fernando De León 17822
Jose Amado Garcia 181469
Edgar Andree Toledo 18439
Ricardo Antonio Valenzuela 18762
Sara Zavala 18893



Parte 1 - Investigación

Digital Signatures

- ¿Qué es?

Las firmas digitales son como huellas dactilares electrónicas. La firma digital asocia de forma segura a un firmante con un documento en una transacción registrada.



- ¿Qué sistemas de llave pública suelen usarse?

Public Key Infrastructure (PKI).

PKI utiliza un algoritmo matemático para generar dos números largos, una clave es pública y una clave es privada.

Digital Signatures

- ¿Existen aplicaciones actualmente?

Si.

Dentro de las aplicaciones más comunes de las firmas digitales podemos mencionar los certificados de distribuciones de software y los correos electrónicos.

- ¿Cómo creen que podría aplicarlo en un ambiente de trabajo?

Se recomienda utilizar firmas digitales cuando se requiere identificar y verificar a las personas, así como también garantizar la integridad del mensaje.

Generalmente esto se puede aplicar en sistemas de mensajería y en la firma de documentos.

Referencias

- <https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq>
- <https://www.iacr.org/archive/crypto2000/18800229/18800229.pdf>
- <https://us-cert.cisa.gov/ncas/tips/ST04-018>