

Módulo 2 Unidad 2

LECCIÓN 1

Sistemas RSA de claves privadas y públicas

Sistemas RSA de claves privadas y públicas

Tiempo de ejecución: 6 horas

Planteamiento de la sesión:

La tecnología ha crecido a medida que el mundo se vuelve cada vez más digitalizado y conectado, la seguridad de la información se ha vuelto de vital importancia. Dentro de este contexto, los sistemas RSA de claves privadas y públicas emergen como pilares fundamentales en la protección de datos sensibles y la garantía de la integridad en las comunicaciones digitales.

El objetivo principal de esta lección es proporcionar a los participantes una comprensión profunda de los sistemas RSA y su aplicación en entornos de seguridad informática. Se adoptará un enfoque integral que combine tanto la teoría como la práctica, permitiendo a los estudiantes adquirir las habilidades necesarias para implementar y gestionar eficazmente estos sistemas en diversos contextos.

A lo largo de la lección, se explorarán los principios básicos de los sistemas RSA, desde la generación de claves hasta la encriptación y la firma digital. Los participantes no solo comprenderán la importancia de estos sistemas en la seguridad de la información, sino que también aprenderán cómo se utilizan en la práctica para proteger datos confidenciales y garantizar la autenticidad de las comunicaciones digitales.

Una parte central de esta lección se enfocará en capacitar a los estudiantes para aplicar los principios de los sistemas RSA en la protección de la información. Se analizarán casos de estudio y escenarios de aplicación práctica para que los participantes puedan comprender cómo se utilizan los sistemas RSA en situaciones reales y cómo pueden implementarse de manera efectiva.



Además, se explorarán las mejores prácticas y medidas de seguridad relacionadas con los sistemas RSA. Desde la gestión segura de claves hasta la implementación de algoritmos de encriptación robustos, los participantes obtendrán una comprensión práctica de cómo proteger la información utilizando sistemas RSA en entornos digitales.

Finalmente, la lección abordará la importancia de la evaluación y la mejora continua en la seguridad de la información. Los estudiantes aprenderán técnicas de evaluación de riesgos y auditoría de seguridad que les permitirán identificar y mitigar vulnerabilidades en los sistemas RSA, garantizando así su eficacia a lo largo del tiempo.

Materiales

- PC con conexión a internet.

