Nombre del alumno:

Ignacio Ivan Sanchez Pantoja

Número de matrícula:

18108365

Nombre del profesor:

# # # #

Nombre del curso:

Arquitectura de Seguridad

Actividad:

Fase #

Fecha:

##/##/####

Índice

Resumen:

Entregables previos:

Actividades realizadas durante las sesiones:

Implementaciones

Introducción a los controles criptográficos de seguridad:

Objetivos del entregable:

El entendimiento del uso de cifrados clásicos como César, Vigenère y Hill, los cuales establecen las bases de la criptografía moderna.

- Se espera que al finalizar el documento se tenga un entendimiento y aplicación del criptoanálisis, utilizando herramientas como el análisis de frecuencias o la prueba de Kasiski para descifrar cifrados clásicos.
- El lector deberá explorar la evolución hacia sistemas más complejos como RSA, entendiendo la aritmética modular y la dificultad de factorizar números primos grandes.
- Se fomenta que el lector analice la vulnerabilidad de los sistemas criptográficos clásicos y modernos ante ataques y criptoanálisis avanzados

Reflexiones personales:

Este documento presenta una perspectiva clara y detallada sobre la evolución de la criptografía, desde sus métodos clásicos hasta los más modernos. Al reflexionar sobre su contenido, es notable cómo las matemáticas, en particular la aritmética modular y el álgebra lineal, juegan un papel fundamental en el diseño y análisis de estos sistemas. Los cifrados clásicos, aunque efectivos en su momento, muestran vulnerabilidades ante técnicas de criptoanálisis avanzadas, lo que demuestra la necesidad de una evolución constante en la seguridad de la información. Por otro lado, la introducción de métodos como RSA marca un salto significativo en la complejidad y seguridad, aunque no estén exentos de riesgos. Esta dualidad entre la seguridad y la vulnerabilidad, siempre presente en la criptografía, refuerza la importancia de seguir innovando en la protección de la información en un mundo cada vez más digital y amenazado por ataques sofisticados.

En el documento se hace uso de una plantilla de Excel donde se realizan todos los procedimientos seguidos durante los algoritmos de cifrado mencionados, es decir, el algoritmo RSA,Hill y cesar.

Anexos:

Plantilla de Excel utilizada:

- CryptografiaRepo/Evidencias de actividades en clase/ejercicio_apicacion_de_cifrados_rsa_hill_vigenere_cesar.xlsx at master · CeramicCodes2/CryptografiaRepo (github.com)

Intercambio de claves por medio del protocolo DiffHellman

Practicas realizadas:

Practica 1:

Objetivos del entregable

- Que el lector identifique los elementos criptográficos dentro de un sistema corporativo simulado aplicando técnicas como AES y 3DES, empleando buenas prácticas y corrigiendo errores comunes en su implementación.
- Que el lector conceptualice los controles criptográficos y su aplicación en la seguridad de infraestructuras corporativas, enfocándose en la transmisión segura de archivos mediante FTP y VPN.
- Que el lector identifique errores comunes en la implementación de controles criptográficos, como la transmisión de datos no cifrados, y aprenda a corregirlos utilizando herramientas como OpenSSL.
- Que el lector aplique los conocimientos adquiridos sobre cifrado y descifrado de datos, realizando recomendaciones basadas en buenas prácticas y estándares, como asegurar la confidencialidad e integridad de la información.

Reflexión personal sobre el documento:

El documento proporcionado muestra una práctica de gran valor para cualquier profesional en ciberseguridad. La aplicación de técnicas de cifrado como AES y 3DES en un entorno simulado no solo ayuda a comprender los aspectos teóricos de la criptografía, sino también a visualizar su importancia en el mundo real. A través de ejercicios prácticos, como la transferencia segura de archivos mediante FTP y el uso de VPNs, se puede notar el impacto de la criptografía en la protección de la información sensible.

Esta experiencia demuestra que la criptografía no es solo una herramienta técnica, sino una estrategia crítica para mantener la confidencialidad y la integridad de los datos en cualquier organización. Además, el enfoque práctico en identificar y corregir errores comunes, como la transmisión de datos no cifrados, subraya la necesidad de estar siempre atentos a posibles vulnerabilidades en la infraestructura. Finalmente, la práctica refuerza la relevancia de dominar estas técnicas para mejorar las medidas de seguridad en el diseño de soluciones corporativas.

Anexos:

CryptografiaRepo/Evidencias de practicas/Practica1SanchezPantoja_ (1).pdf at master · CeramicCodes2/CryptografiaRepo (github.com)

Practica 2:

1. Que el lector identifique los métodos y procesos de cifrado, comprendiendo cómo VPNs, IPSEC y GRE aseguran la transferencia de datos en redes inseguras.

2. Que el lector conceptualice y emplee los diversos métodos de cifrado, explorando la implementación de IPSEC y protocolos como ESP para garantizar la autenticación y el cifrado de los datos.
3. Que el lector haga uso de los diversos métodos de cifrado y análisis matemático, como la autenticación con RSA o PSK y el intercambio de claves con Diffie-Hellman, para mejorar la seguridad en redes corporativas.

---

4. Reflexión personal:

El documento ofrece una valiosa visión sobre la implementación de tecnologías VPN dentro de entornos corporativos y la relevancia de los protocolos criptográficos para garantizar la seguridad de los datos en tránsito. La práctica de configurar una VPN mediante IPSEC y GRE proporciona una comprensión profunda de cómo los datos pueden ser encapsulados y protegidos eficazmente, lo cual es vital en un mundo donde las amenazas cibernéticas están en constante aumento.

Una de las reflexiones más importantes es la relevancia de actualizar y modernizar los sistemas de seguridad, eliminando el uso de tecnologías obsoletas como FTP sin cifrado y adoptando mecanismos más robustos, como HMAC-SHA-256 para la autenticación de datos y AES para el cifrado simétrico. Estos avances garantizan no solo la confidencialidad de la información, sino también su integridad y autenticidad.

Además, la observación de cómo el cifrado simétrico y asimétrico trabajan en conjunto, a través de la implementación de claves públicas y privadas, como RSA y PSK, demuestra la complejidad y sofisticación detrás de los sistemas de seguridad actuales. Esta experiencia refuerza la importancia de entender y aplicar las mejores prácticas criptográficas, no solo para proteger la información, sino también para crear un entorno digital más seguro y confiable.

Practica 3:

Referencias

LOPEZ, M. J. (2011). Criptografia y Seguridad en Computadores. Andalucía: UNIVERSIDAD DE JAEN. Schneier, B. (1996). Applied cryptography: Protocols, algorithms, and source code in C (2nd ed.). John Wiley & Sons. Kahn, D. (1996). The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner

Referencias Azad, A.-S. K. (2015). PRACTICAL CRYPTOGRAPHY. Taylor Francis Group

Galbraith, S. D. (2012). Mathematics of Public Key Cryptography. Cambridge University Press.

Friedman, W. F. (1987). THE INDEX OF COINCIDENCE AND ITS APPLICATIONS IN CRYPTANALYSIS. Laguna Hills, California 92654: AEGEAN PARK PRESS.

Seth James Nielson, C. K. (2019). Practical Cryptography in Python.

Texas: Apress. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*

(3rd ed.). Wiley. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of Applied Cryptography*. CRC Pres

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson. 3. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.

Redes empresariales, Seguridad y Automatización -Introducción. (n.d.). https://contenthub.netacad.com/ensa-dl/6.0.1?lng=es-XL

Email Self-Defense - a guide to fighting surveillance with GnuPG encryption. (n.d.). https://emailselfdefense.fsf.org/en/index.html#step-6