Nombre del alumno:

Ignacio Ivan Sanchez Pantoja

Número de matrícula:

18108365

Nombre del profesor:

# # # #

Nombre del curso:

Arquitectura de Seguridad

Actividad:

Fase #

Fecha:

##/##/####



# Índice

[Índice 1](#_Toc179049798)

[Resumen: 2](#_Toc179049799)

[Entregables previos: 2](#_Toc179049800)

[Entregable previo 1 (Introducción a la Criptografía Clásica) 2](#_Toc179049801)

[Objetivos del entregable: 2](#_Toc179049802)

[Reflexión Personal 2](#_Toc179049803)

[Anexos relacionados: 2](#_Toc179049804)

[Entregable previo 2 2](#_Toc179049805)

[Objetivos del entregable: 2](#_Toc179049806)

[Reflexión personal sobre el documento: 2](#_Toc179049807)

[Anexos relacionados: 2](#_Toc179049808)

[Actividades realizadas durante las sesiones: 2](#_Toc179049809)

[Introducción a los controles criptográficos de seguridad: 2](#_Toc179049810)

[Objetivos del entregable: 2](#_Toc179049811)

[Reflexiones personales: 2](#_Toc179049812)

[Intercambio de claves por medio del protocolo DiffHellman 2](#_Toc179049813)

[Objetivos esperados: 2](#_Toc179049814)

[Reflexión personal: 2](#_Toc179049815)

[Anexos: 2](#_Toc179049816)

[Practicas realizadas: 3](#_Toc179049817)

[Referencias 4](#_Toc179049818)

# Resumen:

# Entregables previos:

Los entregables previos realizados consistieron en 2

## Entregable previo 1 (Introducción a la Criptografía Clásica)

### Objetivos del entregable:

* **Teoría de la Información**: Posterior a la lectura del entregable se espera que el lector tenga una comprensión clara sobre el planteamiento que Claude Shannon introdujo sobre los métodos y estrategias para determinar la seguridad de un criptosistema, utilizando conceptos como entropía, redundancia y mecanismos de confusión.
* **Técnicas de Ocultamiento de Información:**  se espera que el lector entienda las múltiples técnicas de ocultamiento de información que emplean los criptosistemas para asegurar la información, entre las técnicas mencionadas encontramos la **confusión** que no es mas que el ocultamiento de la relación entre el texto claro y el texto cifrado, utilizando métodos como la sustitución, además la **difusión** es otra técnica empleada por los criptosistemas que en este caso diluye la redundancia del texto claro a lo largo del texto cifrado, utilizando métodos como la transposición.
* **La evidente falta de confidencialidad en la antiguedad**: Nació de la necesidad de mantener la confidencialidad de las comunicaciones, especialmente en tiempos de guerra y transacciones comerciales privadas.
* **Problemas Principales de la Criptografía Clásica:** en el documento se exponen algunas de las principales vulnerabilidades de la criptografía clásica, como es la vulnerabilidad al ataques de fuerza bruta, a la aplicación de técnicas de criptoanálisis y el manejo de las claves utilizadas de forma segura

### Reflexión Personal

El documento proporciona una visión detallada de la criptografía clásica, destacando su evolución y los desafíos que enfrentó. La teoría de la información de Claude Shannon y sus conceptos de entropía y redundancia son fundamentales para entender la seguridad de los criptosistemas.

por mencionar un ejemplo, Shannon menciona que un criptosistema es seguro si la cantidad de información obtenida de un conjunto de criptogramas es cero, es decir, si la incertidumbre es infinita, en el documento se plantean definiciones formales como la entropía que López (2011) la define como "el número medio de bits que necesitamos para codificar cada uno de los estados de la variable". Además se expone como las técnicas de confusión y difusión son esenciales para ocultar la relación entre el texto claro y el cifrado, asegurando la confidencialidad de la información, se mencionan temas como la motivación detrás de la criptografía clásica, principalmente la necesidad de mantener la confidencialidad en tiempos de guerra y en transacciones comerciales, resalta su importancia histórica. Sin embargo, los problemas inherentes, como la seguridad limitada por la longitud de la clave y la vulnerabilidad a ataques de criptoanálisis, muestran las limitaciones de estos métodos.

Las máquinas de cifrado, como Enigma y ADFGVX, representan avances significativos en la automatización del cifrado, aunque también demostraron ser vulnerables a los criptoanalistas. Los mecanismos de cifrado clásicos, aunque innovadores en su tiempo, han sido superados por técnicas modernas más robustas y seguras, adaptadas a los desafíos tecnológicos actuales.

En resumen, se expone como la criptografía clásica sentó las bases para el desarrollo de sistemas más robustos, aunque sus limitaciones llevaron a la creación de técnicas modernas más seguras

### Aplicaciones de la información expuesta:

La información expuesta puede servir únicamente con fines ilustrativos/educativos, ya que los cifrados clásicos como tal no tienen una aplicación en la industria moderna, únicamente podría ser utilizado para la de ofuscación de malware que Utilice esta clase de herramientas para poder alterar su firma y dificultar el análisis de malware por medio de la detección basada en firmas.

### Anexos relacionados:

* [CryptografiaRepo/Evidencias de entregables previos/Entregable\_previo1\_Tema1\_Sanchez\_Pantoja.pdf at master · CeramicCodes2/CryptografiaRepo (github.com)](https://github.com/CeramicCodes2/CryptografiaRepo/blob/master/Evidencias%20de%20entregables%20previos/Entregable_previo1_Tema1_Sanchez_Pantoja.pdf)

## Entregable previo 2

**Temas y objetivos:**

### Objetivos del entregable:

1. **Conceptos de criptografía**:
   * **Algoritmos Simétricos**: Utilizados para comunicación 1 a 1, como AES y Triple DES. Su principal reto es la distribución segura de las claves.
   * **Algoritmos Asimétricos**: Como RSA, que resuelven el problema de la distribución de claves mediante el uso de un par de claves públicas y privadas. RSA es robusto y versátil, pero su seguridad depende de prácticas rigurosas y una correcta implementación.
   * **Curvas Elípticas**: Ofrecen una seguridad comparable a RSA con claves de menor tamaño, basadas en problemas matemáticos difíciles de resolver, como el problema del logaritmo discreto.
   * **Protocolos de Intercambio de Claves**: Como Diffie-Hellman, que permiten un intercambio seguro de claves sobre canales inseguros.
2. **Principales máquinas de cifrado utilizadas**:
   * **Máquinas de cifrado clásicas**: Aunque no se mencionan específicamente en el documento, históricamente incluyen dispositivos como la máquina Enigma.
   * **Algoritmos modernos**: AES, Triple DES, RSA, y curvas elípticas.
3. **Principales métodos de cifrado**:
   * **Cifrado Simétrico**: AES, Triple DES.
   * **Cifrado Asimétrico**: RSA, Curvas Elípticas.
   * **Protocolos de Intercambio de Claves**: Diffie-Hellman.

### Reflexión personal sobre el documento:

El realizar ese informe proporciono una visión integral de la evolución y la importancia de los algoritmos criptográficos en la seguridad de las comunicaciones. La distinción entre algoritmos simétricos y asimétricos resalta cómo cada uno aborda diferentes desafíos en la criptografía. Los algoritmos simétricos, aunque eficientes, enfrentan el problema crítico de la distribución segura de claves, lo que subraya la necesidad de protocolos robustos como Diffie-Hellman.

Por otro lado, los algoritmos asimétricos, como RSA, han revolucionado la criptografía al permitir un intercambio seguro de claves y autenticación mediante pares de claves públicas y privadas. Sin embargo, su implementación requiere prácticas rigurosas para evitar vulnerabilidades. La introducción de las curvas elípticas representa un avance significativo, ofreciendo alta seguridad con claves más pequeñas, lo que es especialmente útil para dispositivos con recursos limitados.

En conjunto, estos algoritmos y protocolos no solo protegen la confidencialidad y la integridad de los datos, sino que también aseguran la autenticidad y el no repudio, pilares fundamentales de la seguridad informática. La continua innovación y la adecuada formación en criptografía son esenciales para enfrentar las nuevas amenazas, como la computación cuántica, y garantizar la seguridad de la información en un mundo cada vez más digital y conectado.

### Aplicaciones del entregable:

la información expuesta en el texto sobre criptografía, se puede desarrollar una aplicación de mensajería segura que utilice una combinación de algoritmos simétricos y asimétricos para garantizar la confidencialidad, integridad y autenticidad de los mensajes. De hecho herramientas como GPG hacen pleno uso de cifrados como podría ser AES256 además del uso de cifrados asimétricos como es RSA que generalmente se utilizaría para el intercambio seguro de claves o firmado de datos. Estándares actuales como NIST señalan que es una mejor alternativa hacer uso de curvas elípticas debido al reducido tamaño de sus claves en comparación con RSA, el protocolo Diffie-Hellman para el intercambio seguro de claves en canales inseguros es ampliamente implementado por aplicaciones como Telegram como se define en el **MTProto 2.0**.

### Anexos relacionados:

* [CryptografiaRepo/Evidencias de entregables previos/Entregable\_previo2\_Tema2\_Sanchez\_Pantoja.pdf at master · CeramicCodes2/CryptografiaRepo (github.com)](https://github.com/CeramicCodes2/CryptografiaRepo/blob/master/Evidencias%20de%20entregables%20previos/Entregable_previo2_Tema2_Sanchez_Pantoja.pdf)

# Actividades realizadas durante las sesiones:

Esta sección detallara las actividades realizadas durante las sesiones presenciales, entre estas actividades, podemos destacar el hecho de que se generaron código en Python para poner en práctica tanto el cifrado RSA como el protocolo de comunicación DiffHellman, en un archivo Excel se realizaron procedimientos de cifrado clásicos como puede ser el uso del cifrado Hill, Cesar, Vigenère y RSA.

## 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.

Aplicaciones del contenido:

En el aspecto de los algoritmos de cifra clásica al ser algoritmos vulnerables se aconseja su uso únicamente de forma didáctica para el comprender el funcionamiento de los cifrados actuales mas seguros, algunas aplicaciones pueden realizarse para informar al personal no técnico sobre la importancia de los algoritmos de cifrado y como cada que tengan la oportunidad los empleados deben exigir a los desarolladores el uso de algoritmos de cifrado para brindarles una CIDA es decir Confidencialidad Integridad Disponibilidad y Auditoria a los datos procesados por los sistemas.

En el caso del cifrado RSA y como ya se exploro anteriormente con el caso de Telegram, este puede ser usado para la firma de datos, los métodos de criptoanálisis expuestos ayudaran al personal enfocado en el desarrollo de los sistemas a no seleccionar esa clase de algoritmos para la protección de sus datos.

### 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)](https://github.com/CeramicCodes2/CryptografiaRepo/blob/master/Evidencias%20de%20actividades%20en%20clase/ejercicio_apicacion_de_cifrados_rsa_hill_vigenere_cesar.xlsx)

## Intercambio de claves por medio del protocolo DiffHellman

### Objetivos esperados:

El entregable se propone cumplir con los siguientes objetivos:

* Que el lector identifique y aprenda los métodos de cifrado clave, como RSA y Diffie-Hellman, comprendiendo los fundamentos matemáticos como la factorización y el intercambio de claves.
* Que el lector conceptualice y emplee tanto los algoritmos de cifrado como los patrones de diseño de software (Observer y Template Method), aplicando técnicas de criptoanálisis y comprendiendo cómo se integran en sistemas de seguridad.
* Que el lector haga uso de los métodos de cifrado, analice las vulnerabilidades (por ejemplo, ataques de canal lateral o factorización), y aplique mecanismos adicionales, como el "padding", para proteger la información.

### Reflexión personal:

El documento sobre la implementación del algoritmo RSA y su integración con patrones de diseño de software muestra la importancia de que el lector no solo entienda los algoritmos criptográficos, sino que también sepa cómo integrarlos eficazmente en sistemas escalables. En la era digital, la seguridad de la información depende de la capacidad para desarrollar sistemas robustos que protejan datos sensibles frente a ataques sofisticados. Comprender conceptos matemáticos, como la aritmética modular y la factorización de grandes números, junto con técnicas como el padding en RSA, es esencial para mejorar la seguridad.

Además, la aplicación de patrones de diseño como Observer y Template Method subraya la importancia de una arquitectura sólida para la construcción de sistemas criptográficos. No se trata solo de cifrar y descifrar, sino de saber cómo integrar estos procesos en un entorno práctico, como una API o un sistema de línea de comandos, mientras se mantiene la eficiencia y se minimizan las vulnerabilidades. Esto destaca la necesidad de un enfoque interdisciplinario, donde la criptografía, las matemáticas y el diseño de software se combinan para garantizar la seguridad en un mundo cada vez más digitalizado.

En el entregable se detalla la estructura del sistema, utilizando diagramas UML de clases generados con mermaid, en los anexos se presentará el enlace que conduce al repositorio así como a los diagramas UML.

Además se hace una reflexión sobre las principales diferencias entre el cifrado AES,RSA y ECC, cifrados que sustentan actualmente la seguridad y confidencialidad de los datos en los entornos de TI.

Aplicaciones del contenido:

Este entregable tiene una de las mayores aplicaciones en el ámbito profesional ya que en el documento se proporciona una base sólida para desarrollar una aplicación de seguridad criptográfica que integre los algoritmos RSA y Diffie-Hellman. La propuesta de aplicación se centra en crear una plataforma que permita el intercambio seguro de claves y el cifrado de datos a través de una interfaz web y una interfaz de línea de comandos (CLI). La arquitectura de la solución se basará en patrones de diseño como Observer y Template, asegurando una entrada y salida de datos centralizada y compatible con ambas interfaces.

La implementación de los algoritmos RSA y Diffie-Hellman en Python se realizará utilizando el patrón Template Method, lo que permitirá una estructura modular y adaptable. La aplicación podría contar con un archivo composition\_root de forma similar a la expuesta en el entregable, que gestionará la inyección de dependencias y la generación de instancias de clases necesarias para el funcionamiento del sistema. Además, se puede optar por el uso de adaptadores de entrada y salida para asegurar la escalabilidad y mantenibilidad de la aplicación, como eminentes de la ingeniería de software lo exponen (como es el caso de R.C Martin).

En el documento se explora el desarrollo de una aplicación web utilizando Flask y se explora la implementación de vistas MethodViews para procesar directamente los verbos HTTP como GET y POST. Esto permite que las clases encargadas del cifrado reciban y procesen los datos de manera eficiente. En el documento se exploran mecanismos de seguridad adicionales, como el padding en RSA y la validación de claves en Diffie-Hellman, para proteger contra ataques comunes.

### Anexos:

#### Diagramas UML:

* [CryptografiaRepo/Evidencias de actividades en clase/KRI\_CIPHER/UML\_Diagramas.md at master · CeramicCodes2/CryptografiaRepo (github.com)](https://github.com/CeramicCodes2/CryptografiaRepo/blob/master/Evidencias%20de%20actividades%20en%20clase/KRI_CIPHER/UML_Diagramas.md)

##### Codigo utilizado:

* [CryptografiaRepo/Evidencias de actividades en clase/KRI\_CIPHER/server at master · CeramicCodes2/CryptografiaRepo (github.com)](https://github.com/CeramicCodes2/CryptografiaRepo/tree/master/Evidencias%20de%20actividades%20en%20clase/KRI_CIPHER/server)

##### Comparación entre los diferentes criptosistemas:

* [CryptografiaRepo/Evidencias de actividades en clase/ejercicio comparativos\_Sanchez\_Pantoja.xlsx at master · CeramicCodes2/CryptografiaRepo (github.com)](https://github.com/CeramicCodes2/CryptografiaRepo/blob/master/Evidencias%20de%20actividades%20en%20clase/ejercicio%20comparativos_Sanchez_Pantoja.xlsx)

# 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)](https://github.com/CeramicCodes2/CryptografiaRepo/blob/master/Evidencias%20de%20practicas/Practica1SanchezPantoja_%20(1).pdf)

## 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>

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). *Elliptic Curve Cryptography | CSRC | CSRC*. https://csrc.nist.gov/Projects/Elliptic-Curve-Cryptography

*End-to-End encryption, secret chats*. (n.d.). https://core.telegram.org/api/end-to-end