Nombre del alumno:

Ignacio Ivan Sanchez Pantoja

Número de matrícula:

18108365

Nombre del profesor:

# # # #

Nombre del curso:

Arquitectura de Seguridad

Actividad:

Fase #

Fecha:

##/##/####



# Índice

[Titulo 1](#_Toc170152544)

[Referencias 1](#_Toc170152545)

# Resumen:

# Titulo:

# Entregables previos:

Los entregables previos realizados consistieron en 2

**Puntos Redactados en Base al Documento**

Según lo menciona Lopez fundamentado en la teoría de Shannon, existen dos técnicas básicas de ocultamiento de información, estas técnicas son un concepto clave de cualquier mecanismo de cifrado incluyendo la criptografía clásica:

1. **Confusión**: Trata de ocultar la relación entre el texto claro y el texto cifrado. Esta relación existe y se da a partir de la clave empleada. El mecanismo más simple de confusión es la sustitución, que consiste en cambiar cada ocurrencia de un símbolo en el texto claro por otro. La sustitución puede ser tan simple o tan compleja como queramos.
2. **Difusión**: Diluye la redundancia del texto claro repartiéndola a lo largo de todo el texto cifrado. El mecanismo más elemental para llevar a cabo una difusión es la transposición, que consiste en cambiar de sitio elementos individuales del texto claro.

La criptografía clásica no solo consta del uso de estos mecanismos de cifrado, sino que también involucra la definición del cifrado simétrico. Según Schneier, un criptosistema donde tanto el remitente como el receptor deben compartir la misma clave para cifrar y descifrar los mensajes. Este tipo de cifrado depende completamente de la clave, ya que el algoritmo puede ser conocido públicamente.

**Motivación para el uso de Criptografía Clásica**

La criptografía clásica nació por la necesidad de mantener la confidencialidad de las comunicaciones, ya sea en tiempos de guerra o en transacciones comerciales privadas. Desde la antigüedad, las civilizaciones buscaban maneras de ocultar sus mensajes para que no fueran entendidos por enemigos o terceros no autorizados. La criptografía era, por tanto, una herramienta clave para la seguridad y la privacidad.

**Problemas Principales de la Criptografía Clásica**

1. **Seguridad limitada por la longitud de la clave**: Los cifrados clásicos pueden ser vulnerables a ataques de fuerza bruta, donde un atacante prueba todas las combinaciones posibles de claves hasta encontrar la correcta. A medida que el poder de cómputo ha aumentado, las claves cortas pueden ser fácilmente descifradas.
2. **Vulnerabilidad a ataques de criptoanálisis**: La criptografía clásica, especialmente los cifrados por sustitución y transposición, es susceptible a técnicas de criptoanálisis, como el análisis de frecuencias, que permite deducir el mensaje original a partir de patrones en el texto cifrado.
3. **Distribución y manejo de claves**: Un desafío clave en la criptografía clásica es el manejo de las claves. Para que dos personas se comuniquen de manera segura, deben acordar y compartir una clave de manera segura. En ausencia de medios electrónicos seguros, este proceso es altamente vulnerable a interceptaciones.

**Principales Máquinas de Cifrado Utilizadas**

1. **Enigma**: Fue la máquina de cifrado más conocida, utilizada por los alemanes durante la Segunda Guerra Mundial. Consistía en un conjunto de rotores que intercambiaban letras según configuraciones cambiantes. Aunque era avanzada para su tiempo, fue descifrada por los Aliados, con ayuda de criptógrafos polacos y británicos.
2. **Máquinas de rotores**: Estas máquinas, como la Enigma, utilizaban rotores que sustituían letras basándose en permutaciones complejas. Cada rotor tenía 26 posiciones (correspondientes al alfabeto) y se movía de manera secuencial con cada letra cifrada, creando una secuencia de cifrado que cambiaba constantemente.
3. **ADFGVX**: Fue utilizada por el ejército alemán durante la Primera Guerra Mundial. Combinaba cifrado por sustitución y transposición, haciendo uso de un cuadro polialfabético para generar una secuencia compleja de cifrado. Esta máquina también fue descifrada por criptógrafos aliados.

**Mecanismos de Cifrado Clásicos**

1. **Cifrado César**: Consistía en sumar un 3 a la posición de un determinado carácter, generando un desplazamiento de este. La fórmula utilizada para realizar este tipo de cifrado es:

c = (m + 3) \mod 26c=(m+3)mod26

.

1. **Cifrado Vigenère**: Un tipo de cifrado polialfabético que consiste en el uso de un conjunto de símbolos que actúan como clave la cual se repetirá en múltiples tiempos dependiendo si el texto a cifrar es más grande que la clave.
2. **Cifrado Escítalo**: Utilizado por los espartanos para evitar la captura de información, este cifrado hace uso de la técnica de transposición, alterando el orden de los caracteres que conforman un texto dado.

**Reflexión Personal sobre la Actividad**

La actividad de transcribir y adaptar los puntos sobre criptografía clásica me ha permitido profundizar en los conceptos fundamentales de esta disciplina. He aprendido sobre las técnicas básicas de ocultamiento de información, como la confusión y la difusión, y cómo estas se aplican en diferentes métodos de cifrado. Además, he comprendido la importancia histórica de la criptografía clásica y los desafíos que enfrentaba, como la distribución segura de claves y la vulnerabilidad a ataques de criptoanálisis. Esta actividad ha sido enriquecedora, ya que me ha proporcionado una visión más clara de cómo los métodos de cifrado han evolucionado y la relevancia que tienen en la seguridad de las comunicaciones hoy en día.

## Entregable previo 1

# Actividades realizadas durante las sesiones:

Implementaciones

# Practicas realizadas:

# Anexos:

# Referencias

**No hay ninguna fuente en el documento actual.**