Actividad 4: Herramientas para criptografía y criptoanálisis

Seguridad Informática

Orquidea Seijas

Escuela Técnica Superior de Ingeniería  Grado en Ingeniería Informática

Contenido

[1. Ataque al cifrado de sustitución monoalfabético 2](#_Toc495318162)

[a. Justificación teórica de la base del método de criptoanálisis utilizado. 2](#_Toc495318163)

[b. Descripción de los pasos dados para el ataque. 2](#_Toc495318164)

[c. Texto cifrado a atacar, texto plano recuperado y clave. 2](#_Toc495318165)

[2. Ataque al cifrado de sustitución polialfabético (Vigenère) 2](#_Toc495318166)

[a. Justificación teórica del método de ataque al cifrado de Vigenère. 2](#_Toc495318167)

[b. Etapas seguidas en el análisis 2](#_Toc495318168)

[c. Texto cifrado a atacar, texto plano recuperado y clave utilizada. 2](#_Toc495318169)

[3. Máquina de cifrado Enigma 2](#_Toc495318170)

[a. Justificación sobre la robustez del cifrado Enigma. 2](#_Toc495318171)

[b. Funcionamiento a ambo lados del canal de comunicación la clave de cifrado para el caso de la versión de Enigma I. 2](#_Toc495318172)

# Ataque al cifrado de sustitución monoalfabético

## Justificación teórica de la base del método de criptoanálisis utilizado.

## Descripción de los pasos dados para el ataque.

## Texto cifrado a atacar, texto plano recuperado y clave.

# Ataque al cifrado de sustitución polialfabético (Vigenère)

## Explicación teórica del método de ataque al cifrado de Vigenère.

## Etapas seguidas en el análisis

Descripción de las etapas seguidas en el análisis: número de intentos para establecer la longitud de la clave, número de pruebas para determinar cada una de las letras de la clave, herramientas de ayuda utilizadas.

## Texto cifrado a atacar, texto plano recuperado y clave utilizada.

# Máquina de cifrado Enigma

## Justificación sobre la robustez del cifrado Enigma.

Justificar cómo los distintos elementos (rotores, conexiones, etc.) que intervienen en el cifrado contribuyen a que el cifrado sea más robusto que un cifrado polialfabético convencional como el de Vigenère.

## Funcionamiento a ambo lados del canal de comunicación la clave de cifrado para el caso de la versión de Enigma I.

Explicar cómo se establecía y se compartía entre ambos lados del canal de comunicación (emisor y receptor) la clave de cifrado para el caso de la versión Enigma I (la utilizada por el ejército de tierra y aire alemán durante la II Guerra Mundial).