Herramientas para criptografía y criptoanálisis

Objetivo:

Entender el funcionamiento del cifrado por transposición y sustitución clásicos (cifrado monoalfabético y polialfabético), y tratar de romperlo utilizando técnicas estadísticas.

Comprender el mecanismo de funcionamiento del dispositivo criptográfico “Enigma”.

Recursos:

Herramientas criptográficas desarrolladas por Simon Singh, autor del libro "The Code Book" ("Los códigos secretos" en castellano): http://simonsingh.net/The_Black_Chamber/chamberguide.html

Alternativamente, se pueden utilizar las herramientas de la webhttp://www.cryptoclub.org/tools/ciphers.php

Simulador de la máquina Enigma: por ejemplo, el que se proporciona en la webhttp://users.telenet.be/d.rijmenants/en/enigmasim.htm

Metodología:

En la sección “The Black Chamber” de la web de Simon Singh tenéis información complementaria para el tema “Criptografía Simétrica”. La *Chamber Guide* contiene una explicación detallada de los métodos de cifrado por transposición y sustitución con ejemplos (César, monoalfabético, Vigenère y algunos otros), así como una descripción de las técnicas para atacar estos tipos de cifrado.

1. Ataque al cifrado de sustitución monoalfabético

Usando herramientas para el análisis de frecuencias (por ejemplo, las proporcionadas en Cracking the Substitution Cipher en la citada web, la primera parte de la práctica consiste en intentar descifrar un texto cifrado procedente de un cifrado **monoalfabético aleatorio** (conservando los espacios entre las palabras para hacerlo más fácil, o sin espacios para probar vuestra habilidad), por supuesto sin conocer la clave que se utilizó para cifrarlo.

Alternativamente, podéis utilizar el enlace "Crack a substitution cipher" en la web del CryptoClub, aunque la página de Simon Singh es más completa.

El texto a atacar puede ser uno aleatorio (ficheros de muestra proporcionados por las herramientas), o bien podéis elegir un texto vosotros, cifrarlo, e intercambiarlo con otro compañero que haga lo mismo. En este caso ¡no debéis compartir la clave con el compañero! Dado que la herramienta está pensada para el inglés, es preferible que el texto original esté en ese idioma.

En cualquiera de los dos casos el informe de la sesión debe incluir:

- Justificación teórica de la base del método de criptoanálisis utilizado.
- Descripción de los pasos dados para el ataque: herramientas empleadas, valores de frecuencia utilizados (letras individuales, pares de letras, ...), cuántos intentos han sido necesarios, etc.

- Texto cifrado a atacar, texto plano recuperado, y clave (si la habéis averiguado). Si no la averiguasteis, explicad la causa.

2. Ataque al cifrado de sustitución polialfabético (Vigenère)

La web "The Black Chamber" proporciona también algunos ejemplos y herramientas para intentar romper el cifrado de Vigenère. Esta es una tarea más compleja, pero siguiendo el ejemplo (Cracking the Vigenère Cipher) puede realizarse sin mucha dificultad.

Alternativamente, podéis usar en el "CryptoClub" el enlace "Crack Vigenère":http://www.cryptoclub.org/tools/crack_vigenerecipher.php

Lo mismo que en el caso del cifrado monoalfabético, podéis si lo preferís compartir un texto cifrado creado por vosotros con alguno de vuestros compañeros (sin decirle la clave utilizada). Dado que la herramienta está pensada para el inglés, es preferible que el texto original esté en ese idioma.

En el informe para esta parte debéis incluir:

- La explicación teórica del método de ataque al cifrado de Vigenère.
- 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.

3. Máquina de cifrado Enigma

En este apartado se trata de analizar un poco el funcionamiento de la máquina criptográfica Enigma. Para comprenderla un poco mejor podéis instalar un simulador de la misma. En la web http://www.cryptomuseum.com/crypto/enigma/ se describe el principio de funcionamiento de la máquina Enigma, así como una breve explicación de cómo el método de cifrado empleado fue roto por los aliados durante la Segunda Guerra Mundial, usando la "Bombe". Se proporcionan enlaces a distintos simuladores. Para Windows, podéis usarhttp://users.telenet.be/d.rijmenants/en/enigmasim.htm

Para el informe, se trata de responder a dos cuestiones:

- 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.
- 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).