Criptografía clásica y moderna

Roberto de Miguel García

Criptografía clásica y moderna

septem ediciones

Criptografía clásica y moderna

Septem Universitas

Primera edición: enero, 2008

e-mail: info@septemediciones.com
www.septemediciones.com
Blog: septemediciones.blogspot.com

Diseño cubierta y compaginación: M&R Studio

ISBN: 978-84-96491-79-3
D. L.: M- -2008
Impreso en España- *Printed in Spain*

ÍNDICE

6. CIFRADO SIMÉTRICO O DE CLAVE PRIVADA

7. CIFRADO ASIMÉTRICO O DE CLAVE PÚBLICA CIFRADO ASIMÉTRICO O DE CLAVE PÚBLICA

8. PGP (PRETTY GOOD PRIVACE)

9. APLICACIONES DE LA CRIPTOGRAFÍA

10. CASO PRÁCTICO DE CRIPTOGRAFÍA: EL DNIe

APÉNDICE A: LA CRIPTOGRAFÍA EN LOS NIÑOS

INTRODUCCIÓN

El término criptografía proviene del griego "Kryptos", escondido, y "Graphos", escritura. Es decir, se podría traducir como "Escritura escondida". Se trata de escribir mensajes de tal forma que, otra persona que desee leerlo, no pueda entenderlo, a no ser que conozca cómo se ha escondido.

En la sociedad actual del conocimiento, "información" significa "poder" y "criptografía" es el mecanismo que se utiliza para la protección de la información. Muchos acuerdos internacionales así como el artículo 12 de la Declaración Universal de los Derechos Humanos y el artículo 17 del Convenio Internacional sobre Derechos Políticos y Civiles reconocen el derecho a la intimidad y privacidad como uno de los derechos fundamentales del individuo.

En muchas ocasiones conceptos similares como criptografía, criptoanálisis, criptología y esteganografía son confundidos pero cada uno de estos términos tiene su propio significado.

- Criptografía: Arte de escribir ocultando la información.
- Criptoanálisis: Técnicas utilizadas para descubrir el significado de mensajes encriptados.
- Criptología: Ciencia que abarca el estudio de la criptografía y el criptoanálisis.
- Esteganografía: Proveniente de las palabras griegas "εστεγω" (encubierto) y "γσαφης" (escritura). En la antigua Grecia destaca, en este arte, Demaroto del que se decía que sabía ocultar mensajes de maneras muy originales. Herodoto cuenta la estrategia, que desarrollada por Demaroto, utilizó Histaiaco en la batalla de Salamina cuando el persa Jerjes pretendía sorprender a los griegos: *"Afeitó la cabeza del mensajero, escribió el mensaje en el cuero cabelludo y esperó a que le creciera el pelo. El mensajero pudo viajar sin caer en sospecha. Cuando llegó a su destino se afeitó otra vez la cabeza y se pudo leer el mensaje"*.

La bonanza de un código criptográfico simplemente se basa en lo persistente que sea ante los ataques de técnicas de criptoanálisis. Las técnicas de criptoanálisis se clasifican en función de la información que conoce el criptoanalista:

• *Ataque sólo con parte del texto cifrado*: El criptoanalista solo conoce el texto cifrado. Tanto el contenido, como la cabecera del documento, etc... son desconocidos para él.

• *Ataque con texto original conocido*: El criptoanalista conoce parte del texto original que ha sido codificado. Este ataque es especialmente útil en sistemas de cifrado simétrico por bloques, ya que cada palabra codificada conserva su longitud.

• *Ataque con texto original escogido*: En este caso el criptoanalista conoce el texto cifrado de un texto original escogido por él. Es efectivo para sistemas simétricos y algunos asimétricos.

• *Ataque con texto cifrado escogido*: El criptoanalista es capaz de obtener el texto original de un texto codificado elegido por él. Es el caso menos común de todos.

Existe otra clasificación que sigue como criterio "el modo de actuar del criptoanalista":

• *Ataque con intermediario:* Este ataque consiste en que el cripto-analista se interpone en la comunicación cuando las dos partes están intercambiándose las claves.

• *Ataque de prueba o ensayo (fuerza bruta):* Es el método más simple de todos. Consiste en ir probando cada una de las posibles claves hasta encontrar la que permite descodificar el mensaje. Este método es lento pero con la llegada de los ordenadores e Internet se pueden obtener velocidades aceptables.

Cuando se entra en el terreno de la criptografía militar es justo reseñar a Kerchoffs[1] que estableció las normas que debe cumplir un criptosistema para evitar ser violado por un criptoanalista (siglo XIX). Estas normas son:

• No debe existir ninguna forma de recuperar mediante el criptograma el texto inicial o la clave.

• Todo sistema criptográfico ha de estar compuesto por dos tipos de información:

  – Pública: como es la serie de algoritmos que lo definen.

  – Privada: como es la clave. En los sistemas asimétricos parte de la clave es también información pública.

• La clave escogida debe ser fácil de recordar y modificar.

• El criptograma debe poder ser transmitido usando los medios de comunicación habituales.

• La complejidad del proceso de recuperación del texto original debe corresponderse con el beneficio obtenido.

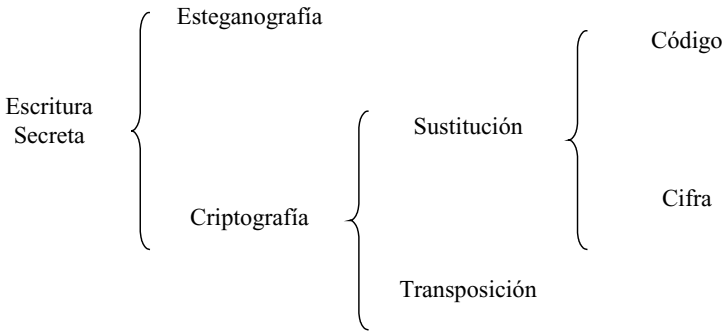

Figura I.1

NOTAS FINALES

[1] **Kerchoffs** (1835-1903):Lingüista y criptógrafo fue profesor de lenguajes en la Escuela Superior de Estudios Comerciales en París durante el siglo IXX. Alcanzó la fama por una serie de dos ensayos publicados en 1883 en *le Journal des Sciences Militaires*. Estos ensayos estudian *el estado del arte* en la criptografía militar.