# Des/Encriptación en la Informática Forense

Plata Cheje Rubén Wismark
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
benhurwk@hotmail.com

**RESUMEN**

En un mundo donde, la información y el conocimiento es lo importante, es necesario cuidar estos aspectos, y es aquí donde entra la seguridad informática y la informática forense

En este artículos se tratará los aspectos referidos a al criptografía y como esta respalda la labor de los expertos forenses informáticos en aras de preservar información importante como evidencias en casos de procesos de Corte.

**Palabras clave**

Criptografia, aoritmos, cifrado, criptosistema.

## 1. INTRODUCCIÓN

La encriptación desde la antigüedad ha sido una forma de proteger la información valiosa; a través de la historia se realizaron infinidad de técnicas, por ejemplo en la segunda guerra mundial

se trabajó con la máquina enigma para transmitir secretos militares.

En la actualidad, la criptografía se suele realizar, tomando en cuenta los estándares internacionales de seguridad y aplicando los distintos tipos de algoritmos criptográficos, entre ellos: RSA, DES, 3DES y AES. Entre estos, se puede sintetizar la combinación de clave pública-privada o asimétrica y la clave simétrica

## 2. CRIPTOGRAFÍA

La criptografía es la ciencia que estudia la transformación de un determinado mensaje en un código de forma tal que a partir de dicho código solo algunas personas sean capaces de recuperar el mensaje original. En general se utiliza para ello una palabra clave o password con la cual se cifra el mensaje, el código resultante solamente puede ser descifrado por aquellos que conozcan el password.

### 2.1. Algoritmos asimétricos o de llave pública

Este es otro factor que se debe tener en cuenta para empezar a trabajar con formulas criptograficas y algoritmos, bueno estos han demostrado su eficacia en entornos de comunicacion inseguros como Internet. Su novedad fundamental es que constan de una pareja de claves unicas, de la que una de ellas se hace publica, y la otra es privada para nosotros. Lo que se cifra con una, se descifra unicamente con la otra, y con este simple concepto jugamos. Un ejemplo muy claro para entender este proceso es el siguiente:

Si A quiere mandarle algo cifrado a B, A le solicita su clave publica a B y cifra el mensaje con ella. De esta forma solo B podrá tener acceso al contenido descifrándolo con su clave privada.

Si A quiere mandarle un mensaje m a B, pero B necesita asegurarse de que realmente viene de A, y que nadie a modificado su contenido, procedemos de la siguiente forma. A genera un hash del mensaje m, H(m), y lo cifra con su privada H(m)Ka. Esto es lo que se conoce como firma digital. Luego A manda el mensaje m, la firma H(m)Ka y su clave publica a B. B descifra H(m)Ka con la pública de A, genera un hash del mensaje original H2(m) y lo compara con el H(m). Si coincide es que todo esta bien.

### 2.2. Algoritmos simétricos o de clave privada.

Los algoritmos simétricos usan la misma llave para encriptacion y desencriptacion (o la llave del desencriptacion se deriva fácilmente de la llave del encriptacion), es decir, la llave para abrir el archivo solo la tiene el destinatario o la persona que lo tenga que recibir, entonces lo que se hace en el proceso es que el remitente o el cifrador coge su mensaje A y lo cifra por medio de una llave publica, cuando lo recibe el destinatario el mensaje A, el lo desencripta con una llave privada que aparentemente solo la tiene él.

## 3. FORMATOS DE FICHEROS

Muchos de los ficheros con lo cuales trabajamos diariamente no son descifrables de manera inmediata. Muchos programas tienen sus propios formatos de fichero, mientras que hay otros que utilizan formatos estándar – por ejemplo, los formatos de fotografías estándar - gif, jpeg, etc.

De manera ocasional, se encuentran ficheros que han sido encriptados o protegidos con alguna contraseña. La complicación que esto presenta varía según la encriptación proporcionada por ciertas aplicaciones, pero puede dar grandes quebraderos de cabeza incluso a entidades como la NSA (o GCHQ o cualquier agencia estatal o local). También existe un gran número de herramientas disponibles en Internet, que se pueden utilizar para romper la encriptación de un fichero. Solo hace falta que se miren alrededor del ordenador con el que se está trabajando, para ver que las personas no son muy

buenas recordando contraseñas y seguramente habrán dejado escrito en algún papel su contraseña. Además, es muy común que las contraseñas estén relacionadas con sus mascotas, familiares, fechas (aniversarios, nacimientos…), números de teléfono, matrículas y otras combinaciones sencillas (123456, abcdef, qwerty...).

Además, las personas son reticentes a utilizar más de una o dos contraseñas para todo, por lo que si consigues una contraseña de algún fichero o aplicación, prueba la misma con otros ficheros porque seguramente será la misma.

Aunque es legal crackear las contraseñas de nuestra propiedad si se han olvidado, en algunos países no es legal intentar resolver cómo se han encriptado los ficheros para protegerlos de ser crackeados.

Las películas DVD también están encriptadas para prevenir que se puedan extraer del DVD y se vendan. Aunque es una manera excelente de encriptación, no es legal buscar métodos para averiguar cómo se ha utilizado la encriptación.

Saber que algo está protegido mediante contraseñas significa aprender cómo abrir ese fichero. Esto es lo que se conoce como "crackear" la contraseña. Buscar información sobre crackers para distintos tipos de contraseñas, es necesario relacionar "cracking XYZ passwords" donde XYZ es el tipo de contraseña que se está buscando.

Si el método de encriptación es demasiado fuerte para romperlo, seguramente será necesario realizar un "ataque de diccionario" o "dictionary attack" (también llamado de "fuerza bruta" o "brute force").

## 4. ¿CRIPTO QUÉ?

La introducción del ordenador (computador), en las oficinas públicas, privadas y nuestros hogares, y la aplicación de estos en el trabajo conjunto o cooperativo a través de las redes de datos, específicamente en Internet, ha popularizado enormemente la utilización de servicios tales como el correo electrónico, mensajería instantánea, transacciones administrativas y financieras y en suma para el envió de información a las personas (familiares, colegas) con las cuales trabajamos o mantenemos algún contacto.

La mayoría de estas personas no saben que es lo que ocurre por debajo de este proceso (enviar información), y lógicamente tampoco debería importarles, pues para ellos, la cuestión es, enviar la información y la otra persona llamémosla Receptor, y con la cual mantiene el contacto reciba esta información, así de sencillo es esto, no importándoles también si la información enviada sea interceptada por algún otro tipo de persona (Intruso), en otras palabras poco les importa la seguridad de la información transferida.

Sin embargo existen personas y entidades, que también utilizan los servicios de una Red (Intranet, Extranet o Internet), que


**Figura 1. El proceso básico de la criptografía**

saben y tienen el conocimiento que la información (su información), que transferirán solo sea conocida y recibida por una persona/entidad autorizada, evitando así las amenazas y riesgos a la que esta expuesta su información.

Y es este tipo de persona/entidad que debería utilizar algún mecanismo que le permita proteger esta información.

Y es aquí donde entra uno de los mecanismos más importantes (sino la mas primordial), para "securizar", la información, la cual se denomina Criptografía.

Otra definición general de lo que es Criptografía es la siguiente: La criptografía es el estudio de técnicas matemáticas relacionadas a aspectos de la seguridad, tales como la confidencialidad, integridad de datos, autenticación, y no repudio.

Una definición más común para la criptografía es: Criptografía es la técnica de convertir un texto en claro (plaintext), en otro llamado criptograma (ciphertext), cuyo contenido de información es igual al anterior pero sólo lo pueden entender las personas autorizadas.

Los términos Cifrar y Descifrar, son utilizados comúnmente para la conversión respectiva, CIFRAR, para convertir el Texto en Claro en Criptograma y DESCIFRAR para convertir el Criptograma en Texto en Claro, y es en esta comprensión de términos que mucha gente, puede entender.

La criptografía en su forma más básica utiliza dos conceptos para su aplicación: La Transposición y la Sustitución, conceptos clave para entender esto de la Criptografía.

La Transposición: Consiste en una reordenación de los elementos básicos (caracteres: letras, números, símbolos).

| F | R | A | T | O | I | P | A | R | G | C | I |
|---|---|---|---|---|---|---|---|---|---|---|---|

del mensaje a cifrar.

| C | R | I | P | T | O | G | R | A | F | I | A |
|---|---|---|---|---|---|---|---|---|---|---|---|

La Sustitución: Que consiste en el cambio de significado de los elementos básicos (caracteres: letras, números, símbolos), del mensaje a cifrar.

| C | R | I | P | T | O | G | R | A | F | I | A |
|---|---|---|---|---|---|---|---|---|---|---|---|

| 3 | E | Z | # | A | T | I | E | T | 9 | Z | T |
|---|---|---|---|---|---|---|---|---|---|---|---|

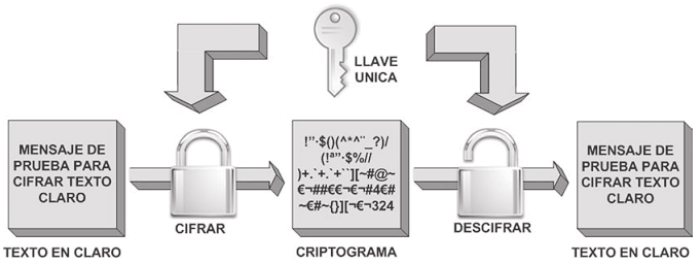


**Figura 2. Encriptación con claves**

Para aplicar estos dos conceptos se utilizan algunos aspectos matemáticos (formulas matemáticas), que nos ayudarán a realizar estas dos tareas, y la aplicación de estas formulas a través de lo que se denomina Algoritmos criptográficos, que nos permitirán cifrar y descifrar los mensajes.

Es aquí donde entra el concepto de Criptosistema. Un Criptosistema es una quíntupla de elementos de la siguiente forma: (m, c, k, e, d)

Donde m representa el conjunto de todos los mensajes sin cifrar (texto en claro).

c representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.

k representa el conjunto de claves que se pueden emplear en el criptosistema.

e es el conjunto de transformaciones de cifrado que se aplica a cada elemento de m para obtener un elemento de c.

d es el conjunto de transformaciones de descifrado, análogo a e.

Entonces todo criptosistema ha de cumplir la siguiente condición: dk ( ek ( m ) ) = m, es decir, que si tenemos un mensaje m, lo ciframos empleando la clave k y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original m.

## 4. ENCRIPTACIÓN BIOMÉTRICA ROBUSTA

La autenticación robusta se basa en la combinación de al menos dos de tres principios de reconocimiento: algo que se sabe (contraseña, usuario); algo que se tiene (tarjeta, flash, dispositivo electrónico) o algo que se es (biometría).

La generación de la clave biométrica es simétrica, lo cual implica falencias en el caso de compartir la llave, ya que este hecho implicaría la posibilidad de hacerse con la clave pública y suplantar la identidad encriptando con la clave biométrica.

Por otro lado, esto se puede subsanar mediante el principio de la autenticación robusta, que solicita que además de utilizar la clave, se aplique una contraseña el momento de la encriptación o desencriptación que sólo el emisor conozca y que comparta sólo con los receptores finales, los cuales la recibirán por otro medio.

Es así, que se tendrá una clave biométrica relativamente

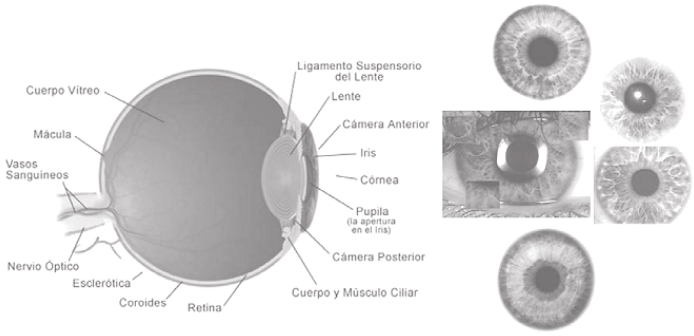


**Figura 3. El iris como elemento biométrico**

robusta frente al hecho de que se puede robar la clave, pero se requerirá a la persona como tal para desencriptarla. Entre los métodos

biométricos sugeridos, se tienen la generación de clave mediante muestra de ADN digitalizado, huella dactilar y finalmente código de Iris.

El ADN es un depósito de información que se trasmite de generación en generación, conteniendo toda la información necesaria para construir y sostener el organismo en el que reside.

La función principal de la herencia es la especificación de las proteínas, siendo el ADN una especie de plano para las proteínas. La estructura del ADN es una pareja de largas cadenas de nucleótidos única para cada ser humano.

Código de Iris: El proceso del Reconocimiento de Iris realizado por el dispositivo biométrico, consta de los pasos de captura de la imagen, localización del iris, optimización de la imagen y clasificación de la imagen.

Huella Digital: Utilizan un escáner que hace rebotar rayos de luz en el dedo, donde un sistema procesa el patrón refractado. Esto permite al lector crear una imagen del dedo, que es trasmitida al software biométrico.

Según un prototipo, para combinar ambas técnicas y realizar así la arquitectura de un software que realiza la encriptación biométrica, para una autenticación robusta con clave pública en sistemas criptográficos avanzados como aquellos que aplican el algoritmo de encriptación AES o el 3DES. Donde:

KPr: Clave privada generada por el algoritmo.

KBio: Clave Biométrica generada por el dispositivo biométrico.

KPu: Clave pública generada por el algoritmo

Generación Clave: Algoritmo de Encriptación (AES, TDES, etc.)

KPuB: Clave pública encriptada por el dispositivo Biométrico.

Como se observa, es posible combinar técnicas de encriptación biométrica y de clave asimétrica; asimismo utilizar un algoritmo veloz de encriptación para el efecto, como lo es el algoritmo AES. La combinación de ambas técnicas de encriptación de mensajes se realizó según el diagrama en

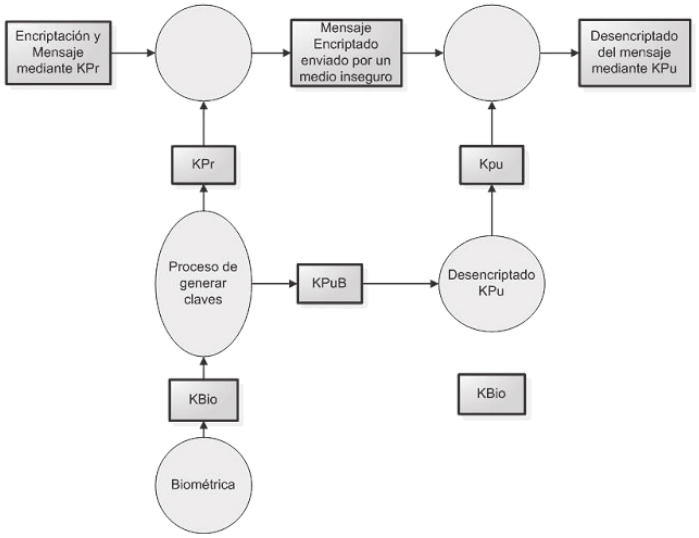


**Figura 4. Prototipo encriptación biométrica**

bloques de la figura anterior donde se muestra el proceso de la generación de claves, ya sean biométricas o la generación de claves pública-privada por otro medio.

Es así que en el transmisor se crea la clave pública biométrica KPuB, que es generada al utilizar la clave pública KPu por un método tradicional, como el algoritmo AES; el emisor encriptará el mensaje a ser transmitido mediante la generación de la clave privada KPr. La clave pública biométrica KBio, será difundida por otro medio y sólo servirá para desencriptar la clave pública biométrica KPuB, no conocida por la entidad que produce la clave

privada, ya que ésta no tendría la clave biométrica.

Por otra parte en el receptor, se reciben tanto la clave biométrica generada por el mecanismo biométrico KBio, como la clave pública encriptada por esta clave biométrica KpuB, denominada clave pública biométrica, es así que en el receptor del mensaje se permitirá finalmente, desencriptar mediante la segunda clave generada.

Por lo tanto, se implementa un algoritmo asimétrico, que cree una clave asimétrica mediante una metodología conocida tanto para la generación de la clave biométrica como para la de la clave asimétrica de cifrado dada; en este caso el algoritmo criptográfico sugerido es AES y como formas de autenticación biométrica se toman las aplicadas mediante: huella digital, código del iris o una clave generada mediante la codificación del ADN del emisor.

Es importante notar que todo este proceso es transparente para el usuario receptor del mensaje, ya que el procedimiento es prácticamente el mismo que la desencriptación de un mensaje firmado.

Asimismo, con la diferencia de utilizar una clave generada por un medio de reconocimiento biométrico, el proceso nuevo es tan simple como el tradicional, para el caso de la encriptación.

El prototipo mencionado fue aplicado y comparado el mismo con otros métodos de encriptación en entornos distintos, de tal manera que se demostró el hecho de que efectivamente es posible incrementar el grado de seguridad de los datos transmitidos en sistemas criptográficos avanzados de clave pública aplicando encriptación biométrica a la clave generada por el algoritmo Rijndael (AES) de manera que solo el receptor pueda autentificar el origen del mensaje recibido.

Las aplicaciones que trabajen con este tipo de autenticación, deben ser amigables y tomar en cuenta que los diseñadores de redes y técnicos no son ni serán los usuarios finales, ya que tanto los sistemas biométricos como el cifrado serán parte de la vida cotidiana en los próximos años.

## 6. CONCLUSIONES

Concluimos aseverando que la encriptación es una excelente manera de resguardar los datos en el disco duro de forma que cualquier intromisión cometida no logre el efecto que quería, robar información. Además la aplicación de rigurosas técnicas de criptografía futuras como es la de tipo biométrica hacen pensar que se augura un auge impresionante a futuro, pero al mismo tiempo se levantan varias cuestionantes alrededor del tema, tales como ¿qué pasaría si la persona que resguarda la información con su clave personal es secuestrada, muerta o simplemente se va de la institución en donde trabaja?. Bueno a seguir investigando y dirimiendo estas cuestionantes del mundo real.

## 8. REFERENCIAS

[1]“Criptografia” Ing. Remberto Gonzales Cruz

[2]“Encriptacion y Biometria” MSc.Ricardo Iván Gottret Ríos

[3]http://www.yanapti.com Segurinfo

[4]http://www.forensic.com/ CriptografiaDesde0/LatinoHack.htm

[5]HHS_es8_Digital_Forensics Cifrado JSE