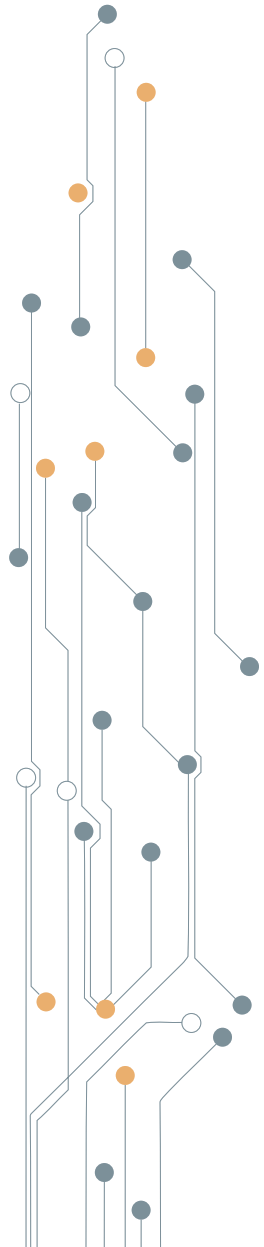
Introducción a la esteganografía

Telefónica EDUCACIÓN DIGITAL

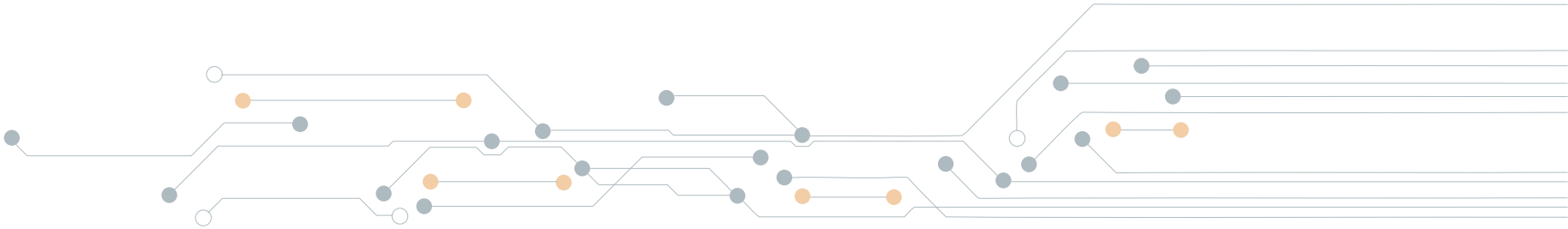
Índice



1. Superando a la criptografía. Limitaciones y retos futuros

La criptografía actualmente tiene tres problemas intrínsecos a su naturaleza. En primer lugar, las comunicaciones cifradas son fáciles de detectar, aunque no por ello seamos capaces de entender lo que se está transmitiendo. Una comunicación cifrada, precisamente por utilizar inteligentemente operaciones para producir confusión y difusión, se diferencia estadísticamente de las comunicaciones en claro; por tanto, un atacante puede detectar cuando este tipo de comunicaciones tienen lugar, localizar a la fuente (máquina o persona que la realiza) y emprender acciones contra la fuente o simplemente inhibir la comunicación. En multitud de escenarios, legítimos o no, el hecho que un atacante conozca que nos estamos comunicando supone un problema práctico, ya sea porque un malhechor está robando datos de una organización (usando criptografía para que no detecten la fuga de información sensible analizando el tráfico en claro), defensores de libertades civiles están intercambiando información en un país dictatorial o agentes infiltrados en una organización terrorista reciben órdenes desde el cuartel general. Por otro lado, está el problema de las claves criptográficas. Su uso, su creación, su almacenamiento y su destrucción suponen el mayor problema de la criptografía moderna.

En la práctica, la mayoría de ataques van destinados a conseguir la clave criptográfica utilizada en una comunicación de una y mil maneras, ya sea infectando el equipo que opera con ella, realizando ataques de escucha física (criptoanálisis acústico, ataques térmicos, estudio del consumo energético, etc.), ingeniería social, etc. Es famosa en el mundo de la criptografía la siguiente frase: *la criptografía no se ataca se esquiva*, haciendo alusión clara que los ataques prácticos en la actualidad van más en la dirección de conseguir las claves en claro que intentar romper los algoritmos, lo cual, hasta lo que se conoce, no es posible con algoritmos modernos.



Ejemplo de criptoanálisis acústico: RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis - **www.cs.tau.ac.il/~tromer/papers/acoustic-20131218.pdf**

En último lugar tenemos el problema de mantener la cadena de privacidad (confidencialidad, integridad y autenticidad) en comunicaciones donde son necesarios elementos intermedios de procesamiento de datos. El mayor ejemplo, y el mayor problema, lo vemos hoy día en la denominada *cloud* (nube) y el *cloud computing*. Si dos personas desean intercambiar información confidencial, pero necesitan que un elemento tercero, por ejemplo, un servicio de Internet, opere sobre sus datos, este servicio necesitará la clave criptográfica para descifrar la información, operar con ella y volverla a cifrar. Imagine el escenario en la que dos delegaciones de un grupo empresarial contratan un servicio externo para hacer estadísticas sobre datos contables que consideran sensibles. No podrán utilizar criptografía en este caso, ya que la tercera parte necesitará la clave criptográfica. Este es un problema que dificulta la privacidad en Internet considerando el potencial de servicios que ofrece la nube y el cloud computing. Quizás en las próximas décadas este problema sea resuelto con un tipo de criptografía, conocida como *criptografía homomórfica completa*, pero aún falta tiempo. Entender las matemáticas que hay detrás de ella no es evidente para cualquier lector, pero en esencia puede verse como aquel tipo de criptografía que permite realizar operaciones matemáticas sobre datos cifrados sin la necesidad de conocer que información está protegida. La ventaja de este tipo de algoritmos es que las operaciones realizadas sobre los datos cifrados re percutirán de la misma manera que si los hubieran realizado en los datos en claro (con la ventaja que no conocen el texto en claro y por tanto la clave criptográfica que los descifra). Por ejemplo, imagine una operación sencilla en la cual se quieren sumar dos números, se desea que una empresa externa sume esos dos números pero que no sepa su valor real. La criptografía homomórfica solucionaría este problema, sumando los datos cifrados y generando un resultado. Al descifrar la información recuperada será igual a como si se hubieran sumado los valores en claro[1].

En este punto existen dos problemas evidentes de la criptografía que hay que trabajar, dificultar la visibilidad de las comunicaciones cifradas (o detectarlas si nos roban información confidencial) y establecer mecanismos para no permitir que las claves criptográficas pudieran ser accesibles. En el interés de proteger mejor las comunicaciones, típicamente cifradas, surgió históricamente, el concepto de la esteganografía.

Este arte, actualmente toda una ciencia, se centra en todo tipo de procedimientos para crear comunicaciones enmascaradas, comunicaciones que pasarían desapercibidas para un potencial atacante. Ni mucho menos la esteganografía es una ciencia novedosa; sin embargo, su aplicación a tantos escenarios variados de nuestras comunicaciones digitales la convierten de facto en un aliado ideal junto a la criptografía, con buenos o malos fines. En la práctica la información, siempre que sea posible, irá previamente cifrada, consiguiendo así un doble nivel de seguridad.

[1] Si desea profundizar en esta nueva criptografía puede profundizar en: https://en.wikipedia.org/wiki/Homomorphic_encryption.

2. Historia de la esteganografía. Conceptos básicos

2.1 | Conceptos básicos y definiciones

La **esteganografía** es la ciencia y el arte de ocultar una información dentro de otra, que haría la función de tapadera o cubierta, con la intención de que no se perciba ni siquiera la existencia de dicha información. A menudo la utilización de esta tapadera o cubierta con fines esteganográficos recibe el nombre de estegomedio. Así, dependiendo de la tapadera que estemos utilizando, hablaremos de estego-imágenes (si se usa una imagen inofensiva como tapadera), estego-vídeo, estego-audio, estego-texto, etc. En teoría, sólo quienes conozcan cierta información acerca de la ocultación, un secreto (típicamente una clave), estarían en condiciones de descubrirla. *En la criptografía, en cambio, no se oculta la existencia del mensaje sino que se hace ilegible para quien no esté al tanto de un determinado secreto, la clave. No obstante, una característica que ambas comparten es que se trata de que un emisor envíe un mensaje que sólo puede ser entendido por uno o varios receptores apoyándose en el hecho de que ambos extremos de la comunicación comparten un secreto específico.*

El término esteganografía, cuyo origen etimológico proviene de las palabras griegas *Steganos* (oculto) y *Graphein* (escribir) **se puede traducir como escritura oculta** y llega a nuestros días como una traducción del término inglés steganography, que a su vez proviene del título del libro *Steganographia*, escrito por el abad alemán *Johannes Trithemius* (1462-1516) en 1499. El libro *Steganographia*, posiblemente el trabajo más famoso del autor, está compuesto por 3 volúmenes, escritos en latín. Los dos primeros recogen procedimientos de escritura oculta, mientras que el tercero, hace referencia a temas mágicos, como astrología o magia negra. Los trabajos de *Johannes Trithemius* son considerados como influyentes en la evolución de la criptografía, así como influyente en la historia de la esteganografía, ya que define sistemas para ocultar mensajes secretos dentro de mensajes aparentemente inofensivos. El libro *Steganographia*, tuvo una circulación reducida en el siglo XVI, concretamente en círculos privados, hasta que se publicó finalmente en 1606.

Independientemente de su origen etimológico, resulta muy complejo datar un origen exacto de las primeras comunicaciones utilizando procedimientos esteganográficos. En muchas ocasiones, las escrituras de civilizaciones antiguas pueden parecer sistemas cifrados e incluso procedimientos de ocultación de mensajes. Sin embargo, es habitual que consistan en lenguas muertas de las cuales se ha perdido la capacidad de interpretación. En otras ocasiones, ha sido posible interpretar el lenguaje, como sucedió con la piedra *Rosetta* y los jeroglíficos. En otras circunstancias, esa incapacidad por comprender una lengua se utilizó como procedimiento criptográfico con utilidad militar. Un caso significativo fue en la II Guerra Mundial donde el ejército norteamericano utilizó indios *navajos* (*codetalkers*) como oficiales de radio.

2.2 | Historia de la ocultación de comunicaciones. Esteganografía clásica

Desde la antigüedad hasta finales del siglo XX (en torno a la década de los 80) se ha documentado el uso de procedimientos de esteganografía clásica o pura. En este sentido, **la esteganografía clásica o pura se puede definir como todo aquel conjunto de métodos de ocultación, que se mantienen en secreto, que permiten esconder un mensaje aprovechándose de un canal específico o tapadera, habitualmente la tapadera utilizada es desconocida para el potencial atacante**. *Se habla entonces de esteganografía pura ya que su seguridad está basada en el desconocimiento, es decir, el atacante no conoce la técnica de ocultación empleada por el emisor ni el medio donde oculta la información deseada.*

Uno de los testimonios más antiguos de uso de esteganografía se remonta al siglo V a.C. Las Historias del historiador griego *Heródoto de Halicarnaso* (484 a.C. – 425 a.C.) recoge en sus crónicas los conflictos entre Grecia y Persia, de especial interés desde el punto de vista de la esteganografía. Según *Heródoto*, fue la escritura oculta lo que permitió a los estados griegos evitar ser ocupada por una Persia opresora. Este hecho queda reflejado en la *historia de Histieo*.

Histieo desde la corte de Persia quería alentar a su yerno *Aristágoras de Mileto* para que se rebelara contra el rey de Persia. Para transmitir sus instrucciones de forma segura, *Histieo* afeitó la cabeza de un mensajero, y tatuó el mensaje en su cuero cabelludo esperando a continuación a que le volviera a crecer el pelo. El mensajero pudo viajar sin levantar sospechas y hacer llegar la información que fue revelada al afeitarse la cabeza. Esta "sutil" comunicación permitió a los griegos percatarse de los planes persas para conquistarlos.

Otra de las crónicas de Heródoto versa sobre la historia de *Demerato*. En esta historia se describe el interés de *Demerato* de avisar a Esparta de que el rey persa *Jerjes* estaba planeando invadir Grecia. Este aviso no fue sencillo. La dificultad, recaía en como enviar el mensaje sin que fuera interceptado por los vigías persas ingeniando para ello un canal de comunicación encubierto. El mecanismo de comunicación consistió en retirar la cera de un par de tablillas de madera, escribir la alerta de la proliferación militar en Persia y luego cubrir el mensaje con cera. Esta tabla, aparentemente en blanco, pasó completamente desapercibida, incluso para sus receptores durante un tiempo, hasta que descubrieron el método tan sutil de comunicación. Como resultado obvio de esta advertencia, los griegos comenzaron a armarse.

Otra de las crónicas relata como el noble *Harpagus* transmitió una información a *Cyrus*, rey de Persia, indicándole que recibiría ayuda desde "dentro" para solucionar la opresión que sufría su país. Para ello vistió a un mensajero de cazador y le proporcionó una libre en cuyo vientre afeitado había escrito el mensaje a transmitir, oculto tras crecer el bello. El cazador con la liebre pasaron desapercibidos. Otros ejemplos similares, se pueden ver en la cultura milenaria China donde se escribían mensajes sobre seda fina, que luego era aplastada hasta formar una pelotita diminuta que se recubría de cera para facilitar que el mensajero ocultara la información tragándose la bola. Pero sin duda, unos de los mecanismos esteganográficos más tradicionales fueron las **tintas invisibles**.

Clásicamente las tintas invisibles son líquidos que se aplican a una superficie concreta y al secarse permiten ocultar a la vista la información escrita. En general, se requiere calor, luz (en la actualidad, infrarrojos o luz ultravioleta) o alguna mezcla química especial para cambiar su color y revelar la información enmascarada. Una referencia clásica a la hora de hablar de tintas invisibles se encuentra en el *siglo I d.c.* El naturalista, escritor y militar romano *Plinio el Viejo* refleja en su obra Historia Natural cómo la leche de la planta *Tithymallus* podía usarse como tinta invisible. Esta sustancia se vuelve transparente al secarse, pero calentándola suavemente se chamusca y se pone marrón. Desde entonces es conocido cómo muchos fluidos orgánicos se comportan de manera similar, muchos de ellos porque son ricos en carbono. De hecho, es posible improvisar tinta invisible con leche, zumo de limón (en general, zumos de frutas), vinagre, vino, azúcar diluida o la propia orina.

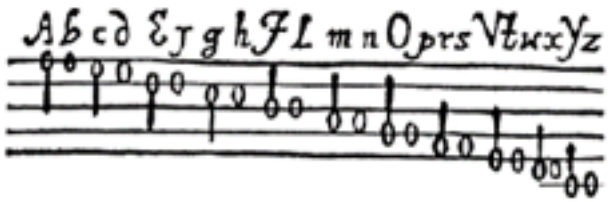
En el *siglo XVI*, el científico italiano *Giovanni Porta* describió una variante curiosa de tinta invisible escondiendo un mensaje dentro de un huevo cocido. El proceso consistía en hacer una tinta con una mezcla de una onza (28 gramos) de alumbre y una pinta de vinagre (la "pinta" inglesa son 568 mililitros), y escribir el mensaje utilizando esta tinta sobre la cáscara. La solución penetra la cáscara porosa y deja un mensaje en la superficie de la albúmina del huevo duro, que sólo se puede leer si se pela el huevo.

Toda esta experimentación en tintas invisibles se fue volviendo muy sofisticada con el paso de los siglos, tanto es así que su uso masivo en conflictos bélicos en el *siglo XX* fue notorio. *Es en el siglo XX donde surge con más fuerza la idea de tintas específicas que idealmente solo reaccionan, se invierten, con un único compuesto químico*. La paranoia que las agencias de inteligencia tenían con las tintas invisibles hizo que durante la II Guerra Mundial, alemanes y estadounidenses comprobaran que todas las cartas que caían en sus manos no contuvieran tinta invisible, lo cual era algo tedioso debido a la diversidad de tipos de tintas y sustancias que debían aplicar para invertirlas. **Fue entonces cuando se avanzó en técnicas de detección basadas en luz ultravioleta**. Todo este conocimiento de tintas invisibles, hoy día, tiene una aplicación civil importante y puede observarse, por ejemplo, en las marcas de agua presentes en billetes de papel moneda o en las tintas ultravioletas.

Pero antes de avanzar a nuestros días, es importante echar un vistazo al avance en procedimientos de ocultación de comunicaciones en los *siglos XVI* y *XVII* como culmen de la cultura renacentista, procedimientos que influirían en otros más modernos ya en los siglos XX y XXI.

Un ejemplo esteganográfico curioso en este periodo tuvo lugar **en la Inglaterra del siglo XVI donde la esteganografía tuvo una gran importancia en las conspiraciones urgidas entre los nobles católicos ingleses que querían destronar a la reina protestante Isabel I (1533-1603) y entregar el trono a la católica María I de Escocia (1542-1587)**. La comunicación entre los conspiradores y la reina María debía pasar lo más desapercibida posible ya que cualquier conocimiento de esta implicaría ser acusados de alta traición y condenados a muerte. Por este motivo, emplearon tanto criptografía como esteganografía para ocultar sus mensajes. *Un mecanismo recurrido fue la ocultación de mensajes en barriles de cerveza que se transportaban sin levantar la atención*.

Muy diferente fue el procedimiento que un siglo después de estos acontecimientos, el científico alemán *Gaspar Schott* (1608-1666) describiría en su libro *Schola Steganographica*. **En esta obra se describía como ocultar mensajes en partituras de música, haciendo equivaler una nota musical concreta con una letra**.



Ejemplo de ocultación en notas musicales y su equivalencia al texto a ocultar

John Wilkins (1614-1672) desarrolló, además, obras relacionadas directamente con el mundo de la criptografía y esteganografía como *Mercury, or The Secret and Swift Messenger* en 1641. **Es destacable el desarrollo de procedimientos para ocultar información utilizando dibujos geométricos, es decir usando puntos, líneas o triángulos de un dibujo para enmascarar información**. Según *Jacqueline L. Tobin* y *Raymond G. Dobard*, autores de la obra *Hidden in Plain View: A Secret Story of Quilts and the Underground Railroad*, ideas de este tipo permitieron a esclavos afroamericanos establecer comunicaciones enmascaradas, aprovechando las tradiciones de su civilización, cultura y religión, desde finales del siglo XVIII hasta por lo menos la Guerra de la Independencia Estadounidense, siglo XIX. A lo largo de los años, los esclavos afroamericanos constituyeron una red encubierta apoyados por familias blancas comprometidas para asistir a los esclavos fugitivos. Se habilitaron casas seguras, estaciones y refugios para ocultarse, al igual que se estableció diferentes códigos secretos de comunicación para facilitar a los esclavos el viaje a la libertad. Uno de los códigos de comunicación oculto consistía en bordar en colchas, en terminología inglesa *quilt code*, una serie de patrones que proporcionaban determinada información. Los captores no veían nada raro en que las mujeres de los esclavos colgaran las colchas al aire libre para airearlas, especialmente en primavera y meses de verano.

Ocultación de información mediante patrón “Bow Tie”.

La simbología de los patrones bordados era muy variada, por ejemplo, proporcionaban la dirección por donde escapar, indicaban si era necesario preparar herramientas para el largo viaje, indicaban si era mejor tomar un camino por la montaña, indicaban si una persona era segura para “hablar”, consejos de no andar en línea recta para evitar rastreos, etc.

Sin duda, la idea de utilizar imágenes para ocultar información ha sido muy socorrida en diferentes momentos históricos. Por ejemplo, en el *siglo XVI* y *XVII*, aprovechando la corriente renacentista de avances en arquitectura, escultura y pintura, se comienza a utilizar imágenes anamórficas, como un mecanismo ideal para camuflar información, sobre todo política.

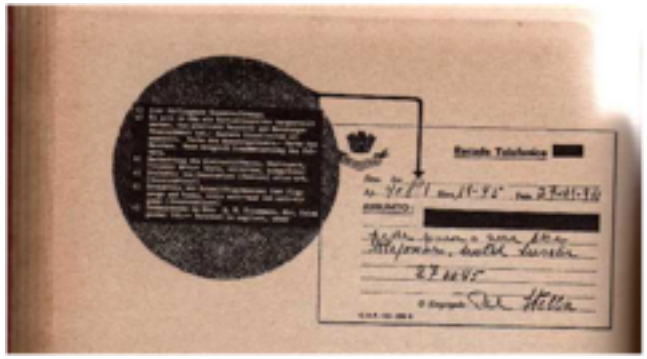
Una anamorfosis, como tal, es una deformación reversible de una imagen a través de procedimientos matemáticos u ópticos, que se manifiesta cuando se observa de una manera especial. Existen multitud de artistas que han plasmado diferentes ideas con imágenes anamórficas. Por ejemplo, *Salvador Dalí*.

Ejemplo de una imagen anamórfica y su significado real

Una imagen anamórfica famosa es el *Vexierbild* creada por *Erhard Schön* (1491-1542) estudiante del famoso artista alemán *Albrecht Dürer*. A primera vista aparecen lugares, costas, barcos y ciudades, pero si se analiza la obra con más cuidado se descubre la composición anamórfica de Carlos V, Fernando I, el Papa Pablo III y Francisco I.

Con el paso de los siglos se comienza a utilizar otro tipo de técnica muy documentada a lo largo de los años, como son los **procedimientos fotográficos para miniaturizar, y por tanto ocultar, información**. En 1857, *Brewster* sugirió la posibilidad de ocultar mensajes secretos mediante reducción fotográfica en un espacio no mayor que un punto de tinta. **Los microfilms hicieron su aparición y técnicas como el micropunto fueron utilizadas con periodicidad (reducir un texto al tamaño de un punto que luego se podía distribuir en una carta, etc.)**.

Imagen anamórfica de Carlos V, Fernando I, el Papa Pablo III y Francisco I



Ejemplo de micropunto oculto en una carta

Los párrafos anteriores son una pequeña muestra de la variedad de procedimientos esteganográficos utilizados en la historia. Se recomienda al lector profundizar en ellos mediante el material adicional proporcionando. En las siguientes páginas se abordarán procedimientos más modernos utilizando las redes informáticas actuales y la capacidad de computación de los ordenadores.

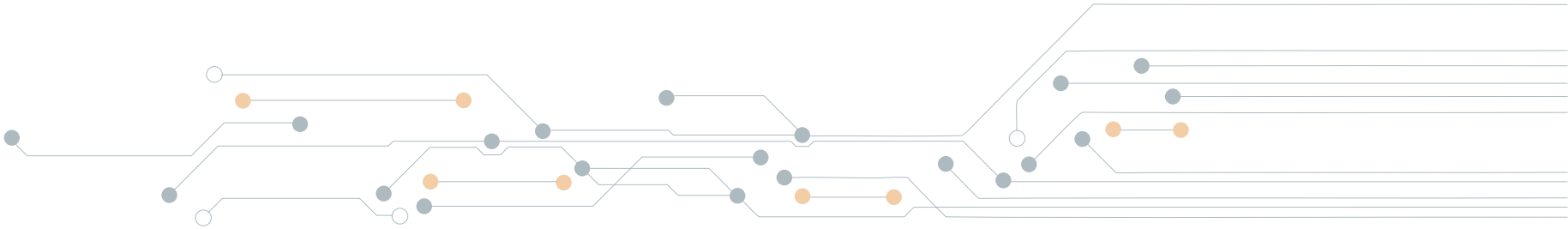
3. Sistemas esteganográficos modernos. Sistemas y tipos

3.1 | Clasificación de sistemas esteganográficos modernos. Portadores

Después de la II Guerra Mundial muchas ramas de la ciencia experimentaron un avance significativo. Los nuevos conocimientos en teoría de códigos (matemáticas), telecomunicaciones e informática, química, física, biología, procesamiento digital de contenido multimedia, etc., tuvieron su reflejo notorio en la ciencia de la esteganografía. Es en esta nueva época cuando se empieza hablar de la ciencia de la esteganografía moderna. Esta nueva vertiente consiste en que la seguridad de los procedimientos esteganográficos no depende de mantener en secreto el algoritmo de ocultación, principios de Kerckhoffs, e incluso tampoco del tipo de la tapadera/cubierta utilizada. La seguridad recae exclusivamente en mantener una pequeña información secreta entre los intervinientes de la comunicación enmascarada, típicamente una clave. Según estos principios, en la actualidad, existen tres tendencias de diseño de sistemas esteganográficos (excluimos en este punto la esteganografía pura):

a. **Estegosistemas de clave simétrica** Es el esquema de estegosistema más común, el que se utiliza en la gran mayoría de herramientas que se analizarán en este curso. Emisor y receptor comparten una clave secreta (estegoclave) y toda la seguridad del sistema se aposenta en ella. Lo normal es que el algoritmo esteganográfico y el tipo de tapadera utilizado sean públicos y un atacante no debería poder detectar ni recuperar la información enmascarada sin la estegoclave.

   De la clave del sistema, estegoclave, pueden derivarse subclaves que se utilizan para cifrar la información a ocultar y tiene utilidad en el proceso de ocultación. Por ejemplo, si el algoritmo esteganográfico modifica bits de los píxeles de una imagen de manera pseudoaleatoria, es común, que subclaves derivadas de la estegoclave primaria alimenten un generador de números pseudoaleatorios del cual se obtienen las posiciones de los píxeles concretos a modificar.



b. **Estegosistemas de clave pública.** Son aquellos sistemas que requieren el uso de dos claves. Una clave pública para el proceso de ocultación y una clave privada para obtener el mensaje oculto. Aunque propuestas más complejas de entender, si el lector desea profundizar en este tipo de estegosistemas se recomienda la lectura de los siguientes artículos:

- *Ahn, L., Hopper, N. Public Key Steganography. Advances in Cryptology, Eurocrypt 2004. pp. 323-341.*
- *Guillon, P., et al. Security and watermarking of multimedia contents. Conference No4, San Jose CA , ETATS-UNIS (21/01/2002), vol. 4675, pp. 38-49. ISBN 0-8194-4415-4.*
- *Backers, M., Cachin, C. Public key steganography with active attacks. Springer Berlin / Heidelberg. LNCS, vol. 3378/2005, pp. 210-226. ISBN: 978-3-540-24573-5.*

c. **Estegosistemas cuánticos.** Estos sistemas aprovechan los conocimientos sobre física cuántica para diseñar sistemas que faciliten la ocultación de información. Existen varias formas de realizar esto, por ejemplo, aprovechándose del ruido cuántico o de los códigos correctores de errores cuánticos. Una introducción recomendada a estos sistemas puede verse en los siguientes artículos:

- *Natori, S. Why Quantum Steganography Can Be Stronger Than Classical Steganography. Springer Berlin / Heidelberg, vol. 102/2006, pp. 235-240. ISBN: 978-3-540-33132-2.*
- *Dobší, M., et al. A Theoretic-framework for Quantum Steganography. Proceedings of Workshop 2006. CTU, vol. A, pp. 124-125. ISBN 80-01-03439-9.*
- *Conti, R., et al. Quantum steganography. Patent 10/849789. 2004.*

Ideas parecidas se han utilizado en las últimas décadas para establecer comunicaciones enmascaradas utilizando diversas características de la naturaleza (comunicaciones atmosféricas con ciertas peculiaridades, ruido ambiente, etc.).

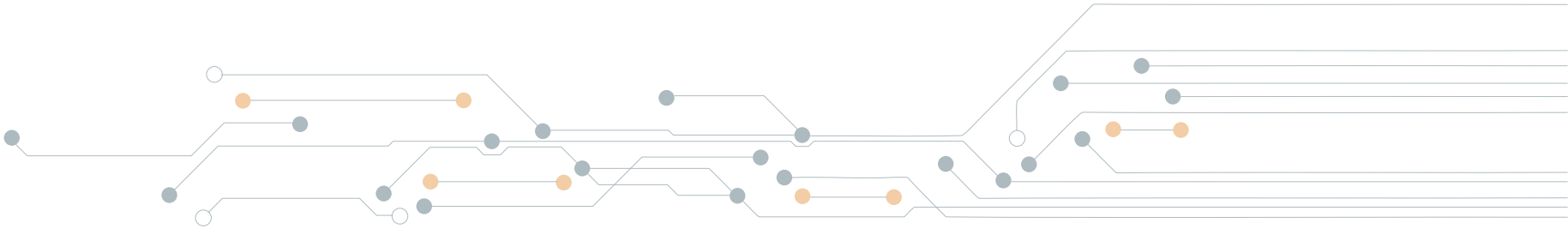
3.2 | Características de un sistema esteganográfico. Diseño y elección

El lector menos avezado no debe preocuparse por esta clasificación, en general, la mayoría de las herramientas disponibles hoy día funcionan con un sistema simétrico. Es decir, emisor y receptor necesitarán compartir una clave para ocultar y detectar la información oculta, y típicamente también se deberán poner de acuerdo en que tipo de tapadera ocultan la información. Por ejemplo, en una imagen digital como un fichero con extensión JPEG, una canción en formato MP3, etc.

En la práctica el interés concreto de un sistema esteganográfico dependerá de 3 características: *capacidad* (cantidad de información que puede ser ocultada), *seguridad/invisibilidad* (probabilidad de detección por un estegoanalista) y robustez (cantidad de alteraciones dañinas que el medio puede soportar antes de que se pierda la información oculta). Considerando estas características la búsqueda de un procedimiento concreto de ocultación en un medio puede ayudarse teniendo en cuenta 3 grandes líneas de creación de algoritmos esteganográficos:

1. La cubierta existe y la ocultación produce alteraciones

Este mecanismo de ocultación es el más habitual en las herramientas que el lector puede utilizar o desarrollar. En esencia, consiste en aprovechar alguna información disponible en una cubierta concreta que puede ser sustituida por otra sin que el receptor de la información advierta ese cambio. Es decir, la información que "machacaremos" puede considerarse en principio como información redundante. A lo largo del curso se observará múltiples ejemplos de este funcionamiento. Sin duda, el más famoso es la ocultación de información en imágenes digitales. Este tipo de técnicas ocultarán información modificando la codificación de los píxeles. Los bits modificados no introducirán variaciones visuales notables en la imagen. A efectos prácticos, el receptor no conocerá la existencia de la información oculta a no ser que disponga de la estegoclave y sepa que cubierta concreta contiene información enmascarada. En ulteriores apartados se analizarán diferentes herramientas que siguen esta filosofía.



2. Generación automática de la cubierta ocultando información en ella

Este procedimiento, quizás no tan común como el anterior, tiene como principio intentar evitar que un emisor utilice una cubierta existente para ocultar información y que el atacante pudiera conseguir la cubierta original, de tal forma que comparando la cubierta original con variaciones de esta (por ejemplo, la creada al modificar la original al ocultar información) se facilitara la detección de la información enmascarada. La idea es sencilla, crear una cubierta nueva para cada comunicación y en el proceso de creación ocultar la información a enmascarar. Por ejemplo, crear una imagen nueva con formato BMP y en el proceso de creación ocultar datos. Como observará el lector en próximos apartados este tipo de técnica ha sido particularmente útil en la creación de estegotextos, textos en lenguaje natural que ocultan información (esteganografía lingüística).

3. La cubierta existe y la ocultación de información no la modifica.

Esta tendencia sin duda es la más particular de todas siendo poco común en las herramientas que el lector conocerá. Tradicionalmente el mecanismo favorito para implementar esta tendencia es la reordenación de elementos. Imagine el siguiente ejemplo, un emisor y un receptor desean intercambiar con esteganografía una clave para ello dispone de 32 imágenes (con 32 nombres de fichero diferentes). La información a transmitir se basa en el orden en el que envíe las imágenes, por ejemplo, en el orden imagen1, imagen7, imagen5, imagen4, imagen3, imagen2, imagen6, etc. Si recuerda sus años de estudiante, las matemáticas le indicarán que existen 32! (2,63130836933 6935301672180121 6e+35) combinaciones posibles con las que enviar las imágenes, por tanto, podrá ocultar jugando con el orden de envío $\log_2(32!) = 117$ bits. Información que podría utilizarse como una clave o semilla criptográfica. En la práctica, la seguridad de este tipo de propuestas recae en mantener en secreto el procedimiento de ocultación y sinceramente no parecen nada prácticas para el envío de cantidades razonables de información (como poco miles de bits). Hoy día, su uso suele estar restringido a procedimientos de ocultación en el envío de paquetes de información utilizando protocolos de comunicación, con la denominada *network steganography*.

Considerando todo lo anterior, la irrupción de las telecomunicaciones e informática ha decantado los procedimientos esteganográficos modernos hacia canales y formatos digitales. Así, en los últimos años se han publicado propuestas de ocultación de información utilizando imágenes, audio y vídeo digital, tecnologías web como cabeceras http o cookies, utilización de la redundancia de las instrucciones máquina en ficheros ejecutables, lenguajes de marcado web como HTML–XML (ocultación basada en caracteres invisibles, modificación de los caracteres de las etiquetas alternando mayúsculas y minúsculas al ser éstas insensitive y ocultación basada en el orden de los atributos de una etiqueta), utilización esteganográfica de diferentes protocolos de comunicación (SOAP, HTTP, TCP, UDP, Ipv4, IPv6, DHCP, ICMP, IPSEC, IGMP, FTP, DNS, 802.2, 802.3, redes inalámbricas, "accesorios" de mails, etc.) para establecer canales encubiertos (*network steganography*) para saltarse protecciones corporativas como, por ejemplo, cortafuegos (típicamente utilizando campos reservados, campos redundantes o el reordenamiento de paquetes), ocultación de información en sistemas ficheros y soportes de almacenamiento, malware oculto en hardware y puertas traseras en microchips, etc.

En próximas lecciones se analizarán brevemente algunas de las técnicas y herramientas más interesantes en la actualidad.

Telefónica EDUCACIÓN DIGITAL