CRIPTOGRAFIA OFENSIVA

Atacando y defendiendo organizaciones

Criptografía aplicada para pentesters, programadores y analistas

Autor: Dr. Alfonso Muñoz

Prólogo D. Raúl Siles

Primera edición

Madrid, España – diciembre 2020

https://www.amazon.es/Criptograf%C3%ADa-Ofensiva-Atacando-defendiendo-organizaciones/dp/B08RB6LGRK

Este libro fue escrito de marzo a diciembre de 2020

en Madrid-España durante una pandemia mundial.

Este libro está dedicado a las almas que se fueron.
Su recuerdo y vida quedarán por siempre.

La esperanza es el único bien común a todos los hombres; los que todo lo han perdido la poseen aún –

Tales de Mileto (624 AC-546 AC)
Filósofo y matemático griego

Hay cosas que sabemos que sabemos.
También hay cosas desconocidas
conocidas,
es decir que sabemos que hay algunas
cosas que no sabemos.
Pero también hay cosas desconocidas
que desconocemos,
las que no sabemos que no sabemos.

— Donald Rumsfeld

Índice de contenidos

Índice de ilustraciones

Prólogo – D. Raúl Siles

El título del presente libro, "Criptografía Ofensiva", enfatiza la estrecha relación existente entre las técnicas de ataque y de defensa, y como bien dice Sun Tzu, "*la mejor defensa es un buen ataque*". Durante los últimos 20 años, pero más especialmente durante la última década al haber aplicado un enfoque más ofensivo y criptográfico en las actividades diarias profesionales que realizo desde DinoSec, he tenido muy presente la importancia de abordar el estudio y análisis de seguridad de cualquier disciplina o tecnología desde esos dos puntos de vista, el ofensivo y el defensivo. Sólo conociendo en detalle las últimas técnicas, herramientas, tácticas y metodologías empleadas por los atacantes se podrá uno defender de manera efectiva y eficiente y, por otro lado, sólo conociendo en detalle el diseño y la implementación de los mecanismos defensivos, se podrá comprender y comenzar la siempre emocionante búsqueda de descubrir como vulnerarlos para evitarlos o anularlos, aplicando una mentalidad *hacker*. Desde el punto de vista del marketing de la industria de seguridad, es lo que hoy en día se conoce como equipos rojo y azul (*red team* y *blue team*), o incluso púrpura (*purple team*), combinando ambas disciplinas o aproximaciones.

Yo siempre he preferido en los cursos técnicos de formación que he impartido a lo largo de mi carrera profesional hacer referencia a esta dualidad mediante el símbolo chino del *yin y el yang*, representando las dos fuerzas opuestas pero complementarias que se encuentran también, en la investigación y análisis de seguridad de cualquier tecnología. La criptología no escapa a esta aproximación tan útil a la hora de comprender en profundidad todos los aspectos que rodean a una disciplina o concepto.

Es importante destacar como, independientemente de qué papel juguemos cada uno profesionalmente (pentesters o hackers éticos, programadores o arquitectos software, analistas, etc.), ofensivo o defensivo, a su vez todos somos también usuarios finales de las tecnologías actuales. De ahí, la importancia de comenzar un libro como este con una muy breve reseña (en el primer capítulo), pero no por ello menos importante, a las buenas prácticas de seguridad, privacidad y criptográficas que todos deberíamos aplicar con rigurosidad y meticulosidad en cada una de nuestras actividades diarias, lo que se suele conocer como seguridad operacional (*operational security*, *opsec,* en inglés).

Os sorprendería conocer algunas de las barbaridades (o "descuidos") que veo constantemente en mi día a día donde el uso correcto de la criptografía brilla por su ausencia, por ejemplo, para la compartición de secretos a través de canales inseguros y/o no controlados, o la compartición de información y ficheros en "la nube" alegremente, incluso en organizaciones internacionales de referencia, o por parte de profesionales o hackers de reconocido prestigio en el sector de la ciberseguridad. Y es que ser constante, meticuloso, disciplinado, fiel a tus ciber-principios y valorar la cultura del esfuerzo, no optando por el camino más corto o sencillo, es algo que parece estar, desafortunadamente, al alcance de muy pocos…

Por eso le animo, por un lado, a ampliar sus conocimientos a través de la lectura de este libro y, por otro, le propongo un reto: aplicar en su día a día esos conocimientos y capacidades de protección sobre todos sus datos y comunicaciones, que se introducen sutilmente en el primer capítulo y se complementan en el resto de los capítulos. Esto le permitirá velar por su seguridad y privacidad, de manera consistente y continua, como usuario final y como profesional, de lo que se beneficiarán sus seres queridos, familiares y amigos, y sus compañeros de trabajo, su empresa u organización respectivamente.

El capítulo dirigido a programadores y arquitectos software es clave para tener claros los fundamentos y principios criptográficos que es necesario aplicar hoy en día desde un punto de vista defensivo, empleados a la hora de la creación de nuevos entornos tecnológicos. A modo de ejemplo, recientemente me he embarcado en una iniciativa centrada en una nueva solución tecnológica donde la criptografía es un elemento clave para su funcionamiento, y donde la correcta aplicación de muchos de los componentes y mecanismos mencionados permiten su apropiado diseño e implementación. Afortunadamente, no se concibe hoy en día el uso de tecnologías sin criptografía si se espera disponer de ciertas propiedades de seguridad y privacidad. Enfatizando que uno no debe de olvidar la historia para no cometer los mismos errores, es igualmente importante adelantarse a los tiempos y prepararse para lo que va a venir. Por ello, el capítulo se complementa con nuevos mecanismos criptográficos que ya se están empleando en la actualidad, y que tendrán incluso más protagonismo en el futuro.

Desde el punto de vista ofensivo, el foco del libro se centra por un lado en un protocolo fundamental en Internet como es TLS, y por otro, en el análisis de mecanismos de autentificación y cracking de contraseñas y credenciales, ambos objetivos comunes de las auditorías de seguridad. Desde un punto de

vista más de investigación y lúdico, se introducen las herramientas de *fuzzing* criptográfico y algunas ideas y herramientas a la hora de resolver retos y desafíos en competiciones tipo *Capture The Flag* (CTF).

Finalmente, el concepto de analista planteado en el libro, un término que puede tener muchas acepciones, hace fundamentalmente referencia a analistas de malware y forenses, donde es común lidiar con especímenes binarios que han sido empaquetados haciendo uso de criptografía para dificultar su estudio, especímenes de *ransomware* cuya funcionalidad principal se basa en la criptografía, o evidencias forenses que deben ser descubiertas tras realizar algún tipo de análisis criptográfico. Como no podía ser de otro modo, dada la pasión del autor por esta disciplina, el capítulo finaliza con el análisis de diferentes canales encubiertos y técnicas de esteganografía de aplicación tanto por analistas, como desde un punto de vista ofensivo.

El lector debe ser consciente de que el libro proporciona un resumen práctico (como bien describe la introducción), lo que informalmente denominaríamos "culturilla general", sobre un área científica y técnica muy compleja como es la criptología, ofensiva (criptoanálisis) y defensiva (criptografía), con una aproximación concisa a múltiples temáticas, y desde diferentes puntos de vista, a través de pequeños apartados de entre una y cinco páginas. Estos breves módulos pretenden captar la atención del lector y se complementan con numerosas referencias para poder profundizar en aquellos temas que le despierten un mayor interés o curiosidad. El libro es un fiel reflejo del estilo del autor, mostrado igualmente en sus presentaciones a través de múltiples conferencias de seguridad a lo largo de los últimos años, que aglutinan un gran número de referencias esperando que el asistente profundice posteriormente en sus contenidos, ávido de adquirir nuevos conocimientos.

El presente libro es, por tanto, un complemento a la certificación profesional de criptografía y protección de la información de CriptoCert que publicamos en 2019 con mucho esfuerzo e ilusión, y ambos presentan un objetivo común: promover y difundir la criptología entre diferentes perfiles profesionales, ya que, quieran o no, todos ellos van a encontrarse con retos criptográficos, defensivos u ofensivos, a lo largo de su trayectoria profesional, y deberán estar preparados para resolverlos con éxito y, sobre todo, no cometer errores graves que les persigan y atormenten durante toda su vida.

Para realmente disponer de conocimientos avanzados en una materia o disciplina es necesario practicar, practicar y, también… practicar. Con este

propósito, además de los ejemplos prácticos en Python, el último capítulo proporciona un conjunto adicional de herramientas (*online* y *offline*), software, recursos, libros y retos o desafíos que le permitirán poner en práctica y "jugar" con los conceptos abordados en capítulos previos. Mi recomendación es que las consulte desde un inicio y las utilice mientras recorre el resto del libro.

Muchos de los aspectos cubiertos por este libro podrían dar (o incluso han dado ya en el pasado) lugar a la elaboración de libros individuales, más específicos y extensos, por lo que este libro debe tomarse como el punto de partida de un largo viaje, que le permita profundizar en nuevos mundos y conocimientos. La criptología, aun presentando unos orígenes clásicos y legendarios, está evolucionando significativa y vertiginosamente hoy en día, por lo que a lo largo del texto se mencionan brevemente numerosas áreas de aplicación con un alto impacto en las tecnologías modernas que utilizamos actualmente, y que utilizaremos en el futuro, como son el cifrado extremo a extremo (E2E), los contratos inteligentes (smart-contracts) o la criptografía postcuántica o ligera (IoT), por tan solo mencionar unas pocas, esperando que el lector profundice, con la inquietud de saber más y ampliar sus conocimientos, en las referencias que acompañan al texto para entrar en más detalle, o incluso para llegar a descubrir tesoros ni siquiera mencionados explícitamente ("*simplemente intentando abrir aún más la mente del lector y mostrarle que muchos otros interesantes mundos le esperan…*"), como especificaciones para el diseño de protocolos criptográficos modernos como el protocolo Noise, empleado por WhatsApp o Wireguard.

Es de agradecer que Alfonso Muñoz dedique su tiempo y esfuerzo a difundir la criptología, a través de libros que, como el que tiene entre las manos (o en su pantalla ;-), o como el ejemplar previo sobre "Seguridad del protocolo SSL/TLS", aglutinan y sintetizan amplios conocimientos, numerosos contenidos y publicaciones, cuya recopilación requiere de muchas horas de análisis y asimilación, destinándose toda la recaudación a una causa solidaria.

Siendo buen aficionado al refranero español, finalizaré con una reflexión sobre un conocido refrán, "*el saber no ocupa lugar*", pero debiendo añadir que adquirir ese saber si requiere de mucho tiempo, esfuerzo, dedicación y práctica. Espero que como lector del presente libro, ponga en práctica todos estos principios a la hora de recorrer sus contenidos y navegar por las múltiples referencias que contiene y que, como buen explorador, amplíe sus conocimientos a través de los nuevos lugares que se le presenten a lo largo del viaje, disfrutando al máximo la aventura.

Raúl Siles es fundador y analista de seguridad senior de DinoSec , compañía especializada en servicios, análisis e investigaciones avanzadas de seguridad, y en formación técnica. Durante 20 años ha aplicado su experiencia en la realización de servicios de seguridad técnicos avanzados y ha innovado soluciones ofensivas y defensivas para grandes empresas y organizaciones en múltiples industrias de todo el mundo. Raúl fue uno de los primeros y de los pocos profesionales a nivel mundial que ha obtenido la certificación GIAC Security Expert (GSE). Más información en www.raulsiles.com (@raulsiles) y www.dinosec.com (@dinosec).

Raúl es también, junto a Alfonso y Jorge, fundador de CriptoCert, ofreciendo la primera certificación técnica profesional de criptografía y protección de la información en español. Más información en www.criptocert.com (@criptocert).

Introducción - ¿Qué no es este libro?

WILL - Lo más triste de todo es que dentro de 50 años
empezarás a pensar por ti mismo, y te darás
cuenta de que solo hay dos verdades en la vida:
uno, que los pedantes sobran, y dos,
que has tirado 150.000 dólares en una educación
que te habría costado un dólar cincuenta por los retrasos
en la biblioteca pública.
CLARK - Sí, pero yo tendré un título, y tú servirás patatas fritas
a mis hijos
WILL - Es posible, pero yo seré una persona de verdad

Matt Damon – El indomable Will Hunting

Cuando era un estudiante a tiempo completo disfrutaba enormemente de la estancia en bibliotecas públicas. A veces se nos olvida el poder de lo público y lo gratuito.

Esa sensación de conocimiento concentrado y esa libertad de descubrir lo que ningún motor de inteligencia artificial podría, descubrir aquel libro que nunca nadie podría recomendarme simplemente porque "no me iba a gustar".

En esa etapa, descubrí un libro que me llamó poderosamente la atención *"La cultura. Todo lo que hay que saber"* de *Dietrich Schwanitz*, una especie de libro sagrado que resumía en un volumen los aspectos más significativos de disciplinas tan variadas como la filosofía, la historia del arte, la música, la historia de Europa, los griegos, la Ilíada, la antigüedad clásica, el renacimiento, la literatura contemporánea. Un libro que, al menos, te permitiría mantener *conversaciones de bar* pareciendo una persona leída y cultivada, y quizás, te permitiera aprender más rápido eliminando información, a priori, ornamental.

Nadie se convierte en un experto en ninguna materia por leer un libro. Lo siento, este libro tampoco lo hará. Pero la capacidad de síntesis de ese libro me pareció significativa y me permitió descubrir aspectos que desconocía y que, en principio, me parecían tremendamente aburridos, y poner foco en otros de manera intensiva.

Llevo tiempo pensando en escribir un libro de criptografía práctica con este objetivo y no tengo claro que sea la aproximación definitiva, pero sin duda, sí la certeza que debe ser escrito.

Durante mucho tiempo, he trabajado en la difusión de material de la disciplina de la criptología, en muchos casos olvidada, bien porque actúa de manera transparente, o bien porque sus fundamentos y bases teóricas requieren un esfuerzo no apto para profesionales perezosos.

Los siguientes capítulos de manera breve y concisa van a reflejar múltiples aristas del uso de la criptografía en el mundo real, en su uso práctico. El texto le permitirá tener una visión global rápida de múltiples disciplinas que hacen uso y necesitan la criptografía, la bibliografía proporcionada le permitirá profundizar en todo el detalle necesario y ampliar y consultar por su cuenta. Precisamente como me sucedió a mí con el libro de Dietrich hace unos años. Encontrará referencias de diferente naturaleza, en español y en inglés, priorizando siempre aquellas de fácil acceso y sin coste. Espero que las disfrute.

Siempre he creído que la criptografía ayuda a construir una sociedad más libre y justa. Quizás este libro ayude en esa dirección.

Dr. Alfonso Muñoz es experto en seguridad informática, área en la que trabaja profesionalmente desde hace 18 años. Su principal actividad se centra en proyectos/tecnologías técnicas avanzadas en seguridad defensiva y ofensiva (Global 500) y su colaboración con organismos públicos. Su especialización se centra en la seguridad ofensiva, la protección de comunicaciones (criptografía y esteganografía) y la investigación avanzada en ciberseguridad.

Su actividad profesional ha sido reconocida con múltiples reconocimientos académicos e industriales, entre ellos por reportar vulnerabilidades en productos de gran uso (Google, Microsoft, etc.). Destaca su perfil divulgador, entre otras áreas, en el área de la criptología. Es co-autor de la red temática Criptored que difunde desde hace más de 20 años millones de documentos y formación online gratuita a todo la comunidad hispanohablante. Es socio de la empresa CriptoCert que proporciona la primera certificación de protección de la información y criptografía en español a nivel mundial. **Twitter: @mindcrypt**

2000 años de criptografía para profesionales perezosos

El sabio no atesora
Cuanto más ayuda a los demás, más se beneficia
Cuanto más da a los demás, más obtiene para él
— Lao Tse

No es sencillo escribir en unos pocos párrafos la importancia que ha tenido para el desarrollo de las diferentes civilizaciones el uso de la criptología[1]. En 1967, el prolijo escritor David Khan, en su magistral obra *The CodeBreakers*[2], recopiló algunos de los hitos de referencia en esta disciplina, un primer acercamiento de "tan solo" 1179 páginas.

Explicar los inicios de esta disciplina, la criptología, no debería ser más complejo que explicar un pequeño juego de colegio. En muchas ocasiones explicado a tal fin con algún cifrador monoalfabético, como el cifrador del César, un mecanismo que modifica las letras de alguna manera predecible, sumando tres posiciones a cada letra (la letra A sería la C, la B la D, etc.). Cualquier alumno aventajado observaría algunos de los males endémicos a la hora de proteger una información con estos mecanismos antiguos, la estadística[3] del lenguaje empleado y el diseño del mecanismo de protección, históricamente solo conocido por emisor y receptor de la comunicación. Durante siglos, en una batalla sin cuartel entre criptógrafos y criptoanalistas[4], se ha intentado minimizar los problemas introducidos por estas características.

La historia demostró que basar la seguridad en mecanismos de protección solo conocidos por emisor y receptor no era una buena estrategia de seguridad, que el tamaño de la información a procesar debería ser de un tamaño relativamente grande para evitar ataques estadísticos (monográmica a poligrámica) y que era útil utilizar una información adicional extra, secreta,

[1] La criptología, del griego κρύπτος (*kryptós*) 'oculto' y λόγος (*logos*) 'estudio', es, tradicionalmente, la disciplina que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas. Se compone de dos disciplinas: la criptografía (se ocupa del estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican) y el criptoanálisis (se ocupa de conseguir capturar criptogramas construidos mediante criptografía sin tener autorización para ello) - https://es.wikipedia.org/wiki/Criptolog%C3%ADa

[2] https://www.amazon.es/Codebreakers-David-Kahn/dp/0025604600

[3] Los lenguajes presentan una gran redundancia, por ejemplo, el inglés o el español. Esto significa que en algunos criptosistemas (básicamente los de tipo clásico orientados al cifrado de caracteres) se puede aplicar esta característica para criptoanalizar textos cifrados

[4] Una referencia excelente para comprender el mundo de la criptografía clásica y su criptoanálisis puede verse en el trabajo de William F. Friedman - https://archive.org/details/nsa-friedman

a modo de clave utilizada de manera inteligente para distribuir las propiedades estadísticas del mensaje (polialfabética).

En 1883, el lingüista holandés Auguste Kerckhoffs en su libro *La cryptographie militaire,* dejó *sentenciado* muchas de estas conclusiones para el diseño correcto de criptosistemas modernos, en lo que se conoce como los principios de Kerckhoffs. Algunos de los más importantes son:

- La seguridad de un criptosistema no debe depender de mantener secreto el algoritmo de cifrado (seguridad por oscuridad). La seguridad sólo debe depender de mantener una pequeña información secreta, la denominada clave de cifrado.

- Si el criptosistema no es teóricamente irrompible, al menos debe serlo en la práctica.

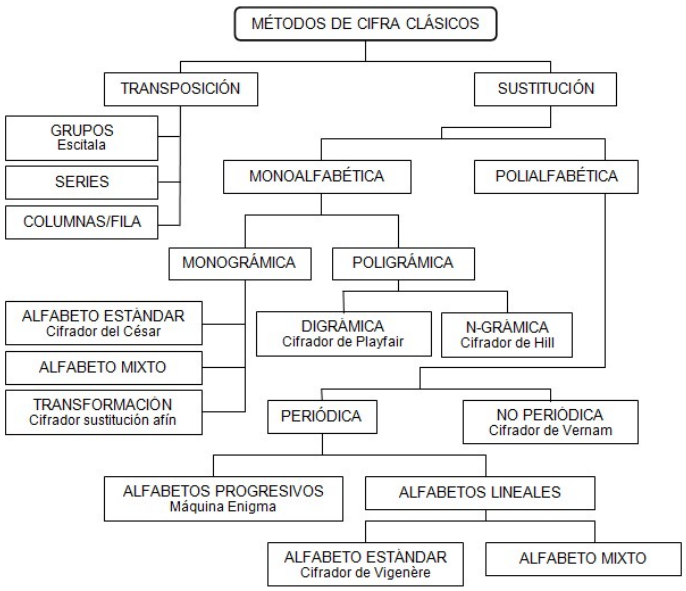

Ilustración 1. Clasificación de los métodos clásicos de cifra y algunos ejemplos

La evolución de las diferentes técnicas de sustitución-transposición, pilar de los criptosistemas, evolucionarían de manera significativa, gracias a avances teóricos en las primeras décadas del siglo XX y al uso militar de máquinas de cifrado[5]-[6], entre ellas la famosa máquina Enigma usada por los alemanes en la II Guerra Mundial. Un hito significativo, en este período, fue en la

[5] Cipher machines - https://www.cryptomuseum.com/crypto/index.htm
[6] https://es.wikipedia.org/wiki/Enigma_(m%C3%A1quina)

década de los 40 con la publicación de dos artículos fundamentales que sentarían las bases de la teoría de la información: *A Mathematical Theory of Communication*, en 1948, y *Communication Theory of Secrecy Systems,* en 1949, desarrollados por Claude Shannon. Estos principios pasarían a conocerse como difusión[7] y confusión[8] y son los pilares de la criptografía moderna. Una criptografía basada en algoritmos públicos cuya fortaleza recae exclusivamente en el conocimiento de la clave criptográfica.

A partir de este momento, la criptografía[9] simétrica experimentaría una evolución sin precedentes, en sus dos modalidades clásicas: la criptografía simétrica de bloques y la criptografía de flujo. En la década de los 70 del siglo XX, la criptografía asimétrica enriquecería aún más el panorama y la utilidad práctica de esta ciencia.

Si se pone el foco en la criptografía simétrica, hoy día y analizando la historia en los últimos 50 años, un lector avezado puede encontrarse multitud de algoritmos simétricos en muchos casos influido por la parte del mundo donde le ha tocado vivir (influencia norteamericana-NIST, Japón, Rusia, etc.). Permítame que le explique brevemente algunos conceptos generales que le serán de utilidad para comprender el diseño y el porqué de muchos de los algoritmos actuales[10].

La criptografía simétrica de bloques es la evolución natural de las técnicas clásicas que en lugar de utilizar sustitución polialfabética y n-gramas evoluciona a bloques de N bits, donde las claves a generar son subclaves de una clave maestra[11].

En esencia, la criptografía simétrica moderna intenta maximizar los dos conceptos fundamentales resaltados por Shannon, la confusión y la difusión. Mediante el mínimo número de operaciones se debe conseguir minimizar el conocimiento del atacante de las propiedades estadísticas del texto en claro y se debe operar el texto de forma que sea ininteligible e irreversible sin el

[7] La difusión define aquellas técnicas que permiten dispersar las propiedades estadísticas inherentes al lenguaje en el texto en claro sobre el criptograma, por ejemplo, mediante permutaciones o transposiciones

[8] La confusión, permitiría generar confusión, caos, mezcla en el resultado cifrado, de tal forma que la dependencia entre texto en claro, clave y criptograma sería lo más compleja posible e impediría romper el algoritmo (propone aplicar la técnica de sustitución).

[9] Es importante no confundir cifrar con codificar - Píldora 6: ¿Ciframos, codificamos o encriptamos? https://www.youtube.com/watch?v=77BrG2vRKss&feature=emb_logo

[10] En adelante, nos centraremos en cuestiones prácticas de su uso, así que le recomiendo le dedique unos cuantos minutos a comprender los siguientes párrafos y le animo a completar su conocimiento con todo el nivel de detalle que desee en la bibliografía recomendada a lo largo de este escrito.

[11] Observará el lector que los algoritmos más importantes en esta disciplina presentan módulos específicos para generación de subclaves, con la clara intención de no revelar información de la clave elegida al atacante, incluso aunque tuviera la capacidad de observar ciertas fases del proceso de cifrado.

conocimiento de la clave, maximizando el efecto avalancha[12]. Por este motivo, el lector verá en los algoritmos más famosos (Triple DES, AES, IDEA, Blowfish, etc.) operaciones y principios comunes como, por ejemplo, el uso de operaciones or-exclusiva (xor)[13], operaciones de desplazamiento o rotación, operaciones de no-linealidad[14] y **estructuras específicas para mezclar las operaciones anteriores**. Un ejemplo famoso de esto es la red o estructura tipo Feistel[15]. La red Feistel recibe su nombre en honor a su inventor Horst Feistel, famoso por su trabajo en IBM por diseños como el algoritmo LUCIFER en la década de los 70 y porque propuestas suyas derivarían en el algoritmo DES, que se convertiría en estándar en 1976 como el algoritmo criptográfico predominante en las comunicaciones mundiales, al menos hasta 1999.

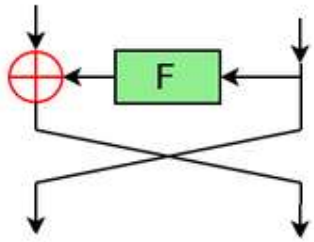

Ilustración 2. La red Feistel coge un bloque de N bits y lo trocea en dos partes. La parte derecha sale como la nueva parte izquierda y la nueva parte derecha será el resultado de hacer una operación or-exclusiva de la entrada izquierda con una serie de modificaciones, función F, de la entrada derecha. Por ejemplo, el algoritmo DES utiliza la red Feistel y la función F realiza funciones de no-linealidad, desplazamientos, or-exclusivas, etc., para facilitar la confusión y la difusión.

[12] Efecto avalancha en el diseño del estándar AES (algoritmo Rijndael) hace que dos vueltas del algoritmo produzcan una difusión completa, en el sentido de que, cada bit del estado depende de todos los bits de las 2 vueltas anteriores, es decir, un cambio en un bit del estado es similar a cambiar la mitad de los bits del estado después de dos vueltas.

[13] Existe un 50% de probabilidad que la entrada que lo produce sea un 1 o un 0. Esto es muy interesante para conseguir difusión y confusión.

[14] Son operaciones matemáticas de no-linealidad, típicamente reflejadas en una serie de tablas a los que, dada una entrada, por sustitución, se produce una salida. Por ejemplo, el algoritmo DES usa funciones de expansión o reducción que genera una salida que al invertir daría igual a varias entradas posibles. El diseño de estas tablas o caja-S es fundamental en la seguridad de los algoritmos de criptografía simétrica modernos. Existen diferentes formas de crearlas, una manera típica es utilizando funciones de Bent.

[15] Aunque este tipo de estructura se ha utilizado en múltiples algoritmos, existen muchas otras opciones, por ejemplo, el actual estándar de cifrado AES no utiliza una estructura Feistel. La información a cifrar se maneja en una estructura de datos, matriz de estado, en la cual se le realizan una serie de operaciones. Es común el diseño de criptosistemas basados en redes SPN (substitution-permutation network) - https://en.wikipedia.org/wiki/Substitution%E2%80%93permutation_network

Una vez definida esta estructura mínima se repetirá un conjunto de operaciones, en los que se suele considerar como número de vueltas[16][17] del algoritmo, hasta que el conocimiento en criptoanálisis y capacidad computacional impida un ataque eficaz contra el algoritmo propuesto e idealmente equivalente a un ataque de fuerza bruta al tamaño de la clave usada.

Por otro lado, la criptografía de flujo es un intento de llevar a la práctica el cifrado de Vernam[18] y el esquema OTP, la única propuesta criptográfica teóricamente irrompible. Recuérdese que el problema práctico del cifrado de Vernam es la distribución de la clave[19]-[20].

Independientemente del modelo de criptografía simétrica que desee utilizar se encontrará con el mismo problema. Cómo proteger y distribuir la clave criptográfica entre las partes de la comunicación de una manera segura. Este problema lo heredamos hasta la actualidad y no existe un mecanismo ideal.

La primera aproximación práctica a este problema se desarrolló a finales de la década de los 70 gracias al artículo *New directions in cryptography*, publicado en 1976 por Bailey Whitfield Diffie y Martin Hellman, que establecía el concepto de criptografía asimétrica o clave pública, en la que cada participante en una comunicación secreta disponía de dos claves, una pública y otra privada. Cualquier emisor podía comunicarse con un destinatario conociendo exclusivamente su clave pública, en tanto que sólo el destinatario podía descifrar la comunicación cifrada, dado que sólo él conocía su clave privada. Es precisamente en este punto donde la criptografía pública tiene un especial interés ya que permite solucionar el problema de la distribución de claves a través de un canal inseguro. La clave pública de un usuario destino (conocida por todos) puede ser utilizada para cifrar una clave, típicamente una clave de sesión simétrica; sólo el destinatario podrá

[16] El algoritmo DES repite 16 veces su estructura Feistel. Por ejemplo, el algoritmo AES, el estándar actual, para un tamaño de bloque de 128 bits y clave 128 bits es seguro frente a ataques como criptoanálisis diferencial o criptoanálisis lineal mediante 6 vueltas. Sus creadores definen el algoritmo con 10 vueltas, 4 más en lo que consideran un posible margen de seguridad.
[17] Too Much Crypto - https://eprint.iacr.org/2019/1492.pdf
[18] https://en.wikipedia.org/wiki/Gilbert_Vernam
[19] Los cifradores de flujo pretenden, utilizando una clave pequeña conocida exclusivamente por emisor y receptor, que exista un generador que en la práctica genere una clave con las propiedades que pudiera encontrarse en un cifrado Vernam-OTP. Lógicamente al tratarse de un procedimiento determinista la secuencia clave generada finalmente tendrá un período, pero en la práctica los cifradores de flujo se pueden diseñar para tener periodos enormes, por ejemplo 10^{38} bits.
[20] Los algoritmos de flujo, aunque con múltiples variantes, en esencia consisten en el diseño de polinomios matemáticos (una función a la que damos valores a las variables en función de una serie de bits iniciales que van variando y que se conocen como semilla), polinomios con una serie de propiedades matemáticas que permiten garantizar propiedades estadísticas y de periodicidad del resultado de dicha función, es decir, de los bits de salida que se utilizarán como clave.

recuperarla porque sólo él conoce su clave privada que deshace la cifra. No obstante, la criptografía pública no es una solución perfecta ya que todavía sufre el problema de garantizar la autoría de la clave pública del receptor/destino de una comunicación. El ataque más común en criptografía de clave pública es un ataque del tipo hombre en el medio, *man in the middle*, es decir, un tercero (atacante) hace creer al emisor de una comunicación que la clave pública del atacante es la del destinatario. Si consigue tal engaño, que en la práctica es muy sencillo de conseguir con herramientas de auditoría clásicas, se interpone en la comunicación de forma transparente pudiendo obtener toda la información a proteger en claro.

En los últimos 20 años se ha intentado poner freno a esta problemática, donde los certificados digitales, las infraestructuras PKI y las autoridades de confianza[21] (CA) juegan un gran rol. Sin olvidar, cómo en muchas ocasiones fabricantes de tecnología han intentado desarrollar e instaurar como estándar de facto soluciones propietarias frente a estos problemas.

La criptografía simétrica y asimétrica, a pesar de sus defectos han sido de gran utilidad en entornos militares, diplomáticos y políticos, hasta la expansión de las redes de comunicaciones e Internet y al uso de la criptografía en las comunicaciones civiles, en el cual influyó notoriamente la publicación de la herramienta PGP por Phil Zimmermann[22] a comienzos de la década de los 90 y los esfuerzos para impedir su uso.

A partir de la década de los noventa, cualquier libro que consulte de la época le dará esa referencia, es común empezar a ver el uso de las diferentes aproximaciones criptográficas en su uso a protocolos de comunicación con naturaleza variada (Kerberos, protocolos esotéricos, etc.).

En cualquier caso, gran parte de este resumen global puede verlo con detalle técnico en muchos de los excelentes libros publicados hasta la época[23]-[24], y, aparentemente esto sería todo. Por suerte para el lector, debe ser consciente del momento excepcional en el que se encuentra esta disciplina (la criptología), abordando problemas heredados de siglos y décadas pasadas y que por primera vez se le intenta dar una solución de un calado cualitativo. Algunas de ellas son:

[21] En pocas palabras verificar la identidad de una clave pública se soluciona incorporando el concepto de tercera parte de confianza. Una tercera parte de confianza es un elemento intermedio que actúa como juez en esa verificación gracias a que mediante el uso de criptografía pública la tercera parte de confianza certificará/firmará la clave pública de cada comunicante.
[22] https://es.wikipedia.org/wiki/Phil_Zimmermann
[23] Applied Cryptography. Bruce Schneier - https://www.schneier.com/books/applied-cryptography/
[24] Handbook of Applied Cryptography – Alfred Menezes et al. - http://cacr.uwaterloo.ca/hac/

- *Criptografía cuántica*. El uso de las propiedades de la física cuántica, como el teorema de no clonación, para crear canales de distribución seguros de claves aleatorias, típicamente simétricas, que no puedan ser interceptadas[25] de manera subrepticia.

- *Criptografía postcuántica.* Diseño de nuevos algoritmos criptográficos resistentes frente a la futura computación cuántica[26].

- *Criptografía homomórfica.* El diseño de algoritmos criptográficos que permiten operar sobre datos cifrados sin necesidad de descifrarlos. Esta disciplina tiene unas implicaciones enormes en la privacidad y en el comercio electrónico al poder facilitar computación de datos privados por terceras partes[27].

- *Lightweight Cryptography[28].* Criptografía ligera diseñada para dispositivos con bajos recursos, especialmente IoT, donde existe un compromiso entre seguridad, rendimiento y coste.

- *Whitebox-cryptography.* Disciplina a medio camino entre la criptografía y procedimientos de ofuscación que tiene como objetivo proteger algoritmos y claves en memoria RAM frente a un atacante que tenga acceso a la misma.

No debe olvidarse que la criptografía es una de las ramas más pesimistas de la ciencia. Asume la existencia de adversarios con capacidad ilimitada de ataque, los cuales pueden leer todos tus mensajes, generar información ilegítima o modificar tus claves aleatorias a su antojo. Curiosamente, también, es una de las ramas más optimistas, mostrando cómo incluso en el peor escenario inimaginable el poder de las matemáticas y la algoritmia puede sobreponerse a cualquier dificultad[29]. O al menos, así es en teoría.

La criptografía[30], al menos desde un punto de vista práctico, no se "ataca" se esquiva. Entender esta afirmación en toda su completitud le permitirá desarrollar y evaluar sistemas reales que utilicen criptografía para su mejor

[25] http://www.criptored.upm.es/crypt4you/temas/cuantica/leccion1/leccion01.html
[26] https://csrc.nist.gov/projects/post-quantum-cryptography
[27] https://homomorphicencryption.org/introduction/
[28] https://csrc.nist.gov/projects/lightweight-cryptography
[29]https://www.premiosfronterasdelconocimiento.es/noticias/fundacion-bbva-premio-fronteras-goldwasser-micali-rivest-shamir-criptografia/
[30] https://github.com/pFarb/awesome-crypto-papers

fortaleza. Espero que los siguientes capítulos le permitan construir esa visión global y verificar sistemas criptográficos de mejor manera.