

CRIPTOGRAFIA OFENSIVA

Atacando y defendiendo organizaciones

*Criptografía aplicada para pentesters,
programadores y analistas*

Autor: Dr. Alfonso Muñoz

Prólogo D. Raúl Siles

Libro completo:

<https://www.amazon.es/dp/B08RB6LGRK>

Primera edición

Madrid, España – diciembre 2020

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.....	10
Prólogo – D. Raúl Siles.....	17
Introducción - ¿Qué no es este libro?.....	22
2000 años de criptografía para profesionales perezosos.....	24
Capítulo 1. Criptografía práctica para usuarios. Protección de datos, privacidad y anonimato.....	32
Capítulo 2. Criptografía práctica para programadores y arquitectos software. Algoritmos y usos.....	36
2.1 Conceptos básicos.....	36
2.2 Criptografía simétrica	37
2.2.1 Algoritmo criptográfico simétrico AES	42
2.2.1.1 Código Python - Cifrando y descifrando con AES-CBC	43
2.2.1.2 Código Python - Cifrando y descifrando con AES-CTR	44
2.3 Criptografía asimétrica o pública.....	45
2.3.1 Algoritmo criptográfico RSA	48
2.3.1.1 ¿Cómo atacar el algoritmo RSA?	50
2.3.2 ElGamal	51
2.3.3 Curvas Elípticas	54
2.3.3.1 ¿Cómo es una curva elíptica y cómo se trabaja con ella?	55
2.3.3.2 ¿Qué curva elegir? ¿Son seguras?	58
2.3.3.3 ¿Cómo cifrar y descifrar información con curvas elípticas? ..	58
2.3.4 Distribución de claves.....	59
2.3.4.1 Distribución de claves criptográficas mediante curvas elípticas. El caso de ECDH	61
2.4 Funciones hash criptográficas.....	64
2.4.1 Ejemplo programación Python de funciones hash criptográficas	

.....	67
2.5 Firma digital	67
2.5.1 Firma digital con curvas elípticas ECDSA	68
2.6 MAC (Message Authentication Code)	72
2.6.1 Ejemplo de programación Python de HMAC-SHA256	74
2.7 Cifrado autenticado.....	74
2.7.1 Ejemplo de programación Python de AES256-GCM	76
2.8 Derivación de claves y password hashing	78
2.8.1 Ejemplo de derivación de clave basada en PBKDF2 con Python	80
2.8.2 Ejemplo en Python de derivación de clave Scrypt.....	83
2.8.3 Ejemplo en Python de derivación de clave basada en Argon2 ...	84
2.9 Generación segura de números aleatorios y pseudoaleatorios	85
2.9.1 Ejemplo de creación de números aleatorios en Python.....	87
2.10 Certificados digitales y codificación X509v3	88
2.10.1 ¿Cómo se usan los certificados digitales en un navegador web? ¿Cómo dificultar la suplantación?.....	92
2.11 Rellenos y padding.....	93
2.12 Computación cuántica. Circuitos cuánticos y corrección de errores cuánticos	96
2.12.1 El algoritmo de Shor y de Grover	97
2.13 Criptografía cuántica y postcuántica	100
2.13.1 ¿Qué contramedidas existen frente a un ordenador cuántico?	102
2.14 Blockchain y criptomonedas.....	105
2.14.1 ¿Cuáles son los fundamentos criptográficos más interesantes?	107
2.14.2 ¿Es posible atacar blockchain o una criptomoneda? ¿Cómo audito su seguridad? ¿Cómo puedo programar de forma segura esta tecnología?	

.....	108
2.14.3 ¿Cómo me formo? ¿Cómo empiezo?	108
2.15 Machine Learning y criptografía	110
2.16 Privacy-Enhancing Technology (PET)	112
2.16.1 Criptografía homomórfica. Computación de datos cifrados... ..	112
2.16.2 Computación multiparte segura y PSI (Private Set Intersection)	116
2.16.2.1 Criptografía umbral. Secreto compartido	118
2.16.3 Cifrado de datos con preservación de formato.....	120
2.16.4 Prueba de conocimiento cero - ZKP	121
2.16.5 Privacidad diferencial.....	122
2.17 Criptografía ligera en Internet of Things (IoT). Lightweight Cryptography	124
2.18 End-to-End (E2E) Encryption. Perfect Forward Secrecy.....	127
2.19 Criptografía y hardware. Almacenamiento seguro de claves	128
2.20 Librerías criptográficas para desarrolladores. ¿Qué algoritmo elegir?¿Cuál es el mejor diseño criptográfico?.....	130
2.20.1 Criptografía y librerías en cloud	131
2.21 Auditoría de código criptográfico. CD/CI y SDLC.....	133
2.22 Identidad digital y JSON Web Token (JWT).....	136
2.23 Criptoanálisis	140
2.23.1 Conceptos útiles para entender los ataques y la robustez criptográfica. IND-CPA, IND-CCA1 e IND-CCA2	140
2.23.2 La criptografía no se ataca, se esquiva.....	142
Capítulo 3. Criptografía aplicada para pentesters y hackers éticos.....	148
3.1 Seguridad criptográfica en las comunicaciones web. SSL/TLS y certificados digitales	149
3.1.1 Ataques criptográficos a los protocolos SSL/TLS	150

3.1.1.1 Ataques basados en compresión y tamaño de petición/respuesta.....	151
3.1.1.2 Ataques basados en implementaciones incorrectas y mal uso de algoritmo	153
3.1.1.3 Ataques basados en downgrade y flujo del protocolo	160
3.1.1.4 Ataques basados en relleno/padding.....	161
3.1.1.4.1 ¿Cómo proteger el padding de una comunicación? El caso de Lucky13	164
3.1.1.5 Ataques a TLS 1.3	167
3.1.1.6 Lecciones aprendidas en ataques criptográficos a TLS/SSL	172
3.1.2 Certificados digitales. Fuga de información y fingerprinting...	174
3.2 Cracking de contraseñas y suplantación de autenticación.....	180
3.2.1 <i>Basics</i> y recomendaciones.....	180
3.2.1.1 Atacando e identificando. Fuerza bruta, colisiones y codificación.....	181
3.2.1.2 Aplicaciones de cracking. John The Ripper y Hashcat	182
3.2.2 Creación y expansión de diccionarios de cracking de contraseñas	184
3.2.3 Credenciales en sistemas operativos. Cracking y evasión de autenticación.....	187
3.2.3.1 Sistema operativo Microsoft Windows	187
3.2.3.2 Sistema operativo Linux y MAC.....	192
3.2.4 Evasión de autenticación online y autenticación basada en contraseña.....	193
3.2.4.1 Ataque a la autenticación en protocolos basada en contraseña	193
3.2.4.2 Client-side attacks. Captchas, tokens JWT y TOTP.....	196

3.2.4.3 Burp suite y extensiones. Atacando la criptografía y bypass autenticación	198
3.2.5 Cracking de credenciales de software de cifrado y secure password storage.....	200
3.2.6 Cracking de credenciales en documentos ofimáticos y certificados digitales.....	201
3.2.7 Cracking de credenciales en comunicaciones inalámbrica	205
3.3 Fuzzing en criptografía y tecnologías blockchain. Detectando implementaciones incorrectas y vulnerabilidades	210
3.4 Herramientas para CTF (Capture the flag). Criptoanálisis y estegoanálisis	213
Capítulo 4. Criptografía para analistas.....	215
4.1 Criptografía y malware. Ransomware y cryptojacking.....	216
4.2 Forense criptográfico. Extrayendo credenciales.....	221
4.3 Esteganografía y canales encubiertos. Pentester, analistas y forenses	225
4.3.1 Esteganografía en la actualidad. Definición de conceptos.....	225
4.3.2 Clasificación de sistemas esteganográficos modernos. Portadores	227
4.3.3 Técnicas esteganográficas en la actualidad.....	230
4.3.3.1 Ocultación de información en imágenes digitales	231
4.3.3.1.1 Ocultando con Digital Invisible Ink Toolkit	231
4.3.3.1.2 Ocultación en imágenes JPEG con F5	234
4.3.3.1.3 Ocultación en imágenes PNG. El caso de Invoke-PSImage	236
4.3.3.1.4 Stegosploit, polyglots y APT-Modernos. Stegomalware en imágenes digitales	237
4.3.3.2 Ocultación de información en audio digital	240

4.3.3.3 Ocultación en sistemas de ficheros y formatos	243
4.3.3.4 Esteganografía en código interpretado. Lenguaje HTML y XML.....	249
4.3.3.5. Canales encubiertos en protocolos de comunicación. Network steganography	251
4.3.3.5.1. Canal encubierto en TCP mediante número inicial de secuencia. Ejemplo con Covert-tcp.....	254
4.3.3.5.2. Canal encubierto en DNS. Mística – La navaja suiza.	256
4.3.3.6. Herramientas de estegoanálisis. Detección práctica de información oculta con esteganografía.....	257
Capítulo 5. Formación continua en criptografía. Libros y recursos.....	260

Índice de ilustraciones

Ilustración 1. Clasificación de los métodos clásicos de cifra y algunos ejemplos.....	25
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.....	27
Ilustración 3. Web oficial proyecto PRISM Break.....	34
Ilustración 4. Esquema de cifrado simétrico	38
Ilustración 5. Esquema de cifrado en flujo. Generador de claves basado en una semilla genera bits que serán aplicados al texto a proteger mediante una función or-exclusiva (xor).....	38
Ilustración 6. Cifrado y descifrado con modo CBC y CTR.....	40
Ilustración 7. El modo de cifrado ECB permite recuperar información sin necesidad de anular el algoritmo criptográfico o conocer la clave. Su debilidad reside en repetir el cifrado de bloques idénticos	40
Ilustración 8. Modo de cifrado GCM.....	41
Ilustración 9. Estructura del algoritmo criptográfico AES.....	43
Ilustración 10. Generación de claves RSA con el software educativo genRSA	49
Ilustración 11. Ejemplo de expresiones analíticas para suma de dos puntos en una curva. $P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3)$	56
Ilustración 12. Ejemplo de expresiones analíticas para multiplicación de un punto $R(x, y)$	57
Ilustración 13. Visualización de los puntos de una curva elíptica	58

Ilustración 14. En la tabla puede observarse la longitud de clave recomendada en función del tipo de criptografía utilizada. Es importante resaltar cómo para una misma seguridad en criptografía de clave pública las claves en criptografía de curvas elípticas son significativamente menores. Por ejemplo, la seguridad de una clave de 2048 bits en un algoritmo asimétrico basado en la dificultad de factorización de un producto de números primos, como es el caso del algoritmo RSA, sería equivalente a una clave de 224 bits en un algoritmo asimétrico basado en curvas elípticas. La diferencia en tamaño es sustancial. Fuente: Cryptographic Key Length Recommendation. URL: <https://www.keylength.com/en/4/#Biblio4>..... 60

Ilustración 15. Curva $y^2=x^3+33x+51 \pmod{71}$ con orden de la curva $n=67$ (número de puntos que hay en la curva) y elemento generador el punto $G=(57,18)$ – <https://grau1.de/code/elliptic2> 63

Ilustración 16. Cálculo en Python del hash criptográfico SHA-256, SHA3-256, BLAKE2s y RIPEMD-160 67

Ilustración 17. Creación y validación de MAC..... 72

Ilustración 18. Cifrado autenticado - https://en.wikipedia.org/wiki/Authenticated_encryption..... 73

Ilustración 19. Ejemplo de uso de la herramienta CyberChef del GCHQ para calcular un HMAC-SHA256 74

Ilustración 20. Modo de cifrado autenticado AES-GCM..... 75

Ilustración 21. Ejemplo de programación en Python de AES-GCM 77

Ilustración 22. Recommendation for Password-Based Key Derivation Part 1: Storage Applications. NIST. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132> 80

Ilustración 23. Algoritmo y diagrama general de funcionamiento de PBKDF2. La entrada se trocea en bloques múltiples del tamaño del hash. Si

kLen=hLen solo existirá una fila. El valor final se calculará como el xor de todas las iteraciones anteriores.....	81
Ilustración 24. Ejemplo de uso de la herramienta CyberChef del GCHQ para cálculo de PBKDF2.....	82
<i>Ilustración 25. Programación en Python de KDF script y ejemplo de análisis de duración de tiempo</i>	<i>84</i>
Ilustración 26. Estructura de un certificado X.509v3	89
Ilustración 27. Ejemplo de certificado X.509 y como se puede ver en un navegador web.....	91
Ilustración 28. Generación de certificado auto firmado con OpenSSL	91
Ilustración 29. Validación de la fecha de expiración de un certificado digital desde consola con OpenSSL	91
Ilustración 30. Mecanismos de relleno de bits con utilidad, no sólo, en criptografía: X.923, ISO 10126, PKCS#7, etc. https://en.wikipedia.org/wiki/Padding_(cryptography)	94
Ilustración 31. Ejemplo de ciphertext-stealing sin relleno. Seleccionando cuidadosamente los 2 últimos bloques de salida es posible realizar un proceso inverso para recuperar la información en claro sin necesidad de relleno. La clave en este punto es el XOR del último bloque, al tratarse de una operación que actúa a nivel de bit nos permitirá recuperar solo el trozo que necesitamos e ignorar el resto – Fuente: https://en.wikipedia.org/wiki/Ciphertext_stealing-	95
Ilustración 32. Número de cúbits estimados para anular la criptografía actual. Datos basados en el informe Quantum Computing: Progress and Prospects (2019) y Capítulo 2 - Criptografía en el mundo real (Gonzalo Álvarez Marañón).....	99
Ilustración 33. Evaluación temporal de uso de la criptografía postcuántica en función de la validez temporal de una información -	

https://i.blackhat.com/eu-20/Thursday/eu-20-Gagliardini-Quantum-Security-And-Cryptography-Youre-Probably-Doing-It-Wrong.pdf	104
Ilustración 34. Estructura de árbol de Merkle en la validación de un bloque en bitcoin. Fuente: https://btc-investor.net/wp-content/uploads/2018/09/Merkle-Tree-Hashing-How-Blockchain-Verification-Works-1.png	106
Ilustración 36. Comparación de algunos de los esquemas SWHE más famosos.....	114
Ilustración 37. Operaciones permitidas en librerías y algoritmos criptográficos con uso homomórfico	115
Ilustración 38. Ejemplos de algoritmos criptográficos ligeros recogidos en la literatura.....	126
Ilustración 39. Métricas habituales analizadas para el diseño o uso de algoritmos criptográficos ligeros.....	126
Ilustración 41. Funcionamiento de los elementos de XACML - https://es.wikipedia.org/wiki/XACML	138
Ilustración 42. Funcionamiento de SAML.....	138
Ilustración 43. El protocolo TLS en realidad se compone de diversos protocolos que ayudarán en la protección de la información	150
Ilustración 44. Ejemplo de inyección de código JavaScript en el ataque Sweet32	155
Ilustración 45. Cifrado de bloque en modo CBC.....	157
Ilustración 46. Esquema visual del ataque BEAST	158
Ilustración 47. Ejemplo de adivinación de cookies con BEAST	159
Ilustración 48. Ejemplos de codificación de padding al final de una información	161
Ilustración 49. Bleichenbacher padding oracle attack	163
Ilustración 50. Esquemas de cifrado autenticado.....	165

Ilustración 51. Proceso de cifrado (DTLS)	166
Ilustración 52. Esquema general de ataque 9 lives of Bleichenbachers cat	169
Ilustración 53. Proceso completo de ataque a TLS 1.3 con 9 lives	170
Ilustración 54. Resumen de ataques de padding a implementación TLS/SSL modernas	171
Ilustración 55. Conclusiones de la investigación de ataques en TLS publicados en mi ponencia – Reversing Cryptographic attack over SSL/TLS - https://www.youtube.com/watch?v=m1Gwi6jKPCE	173
Ilustración 56. Herramienta para intentar deducir del tamaño de una información con qué algoritmo fue protegida - https://tools.kali.org/password-attacks/hash-identifier	181
Ilustración 57. Ejemplos de uso de Crackmapexec para conexión remota a equipos.....	189
Ilustración 58. Ejemplo de herramienta Kerbrute para realizar ataque de fuerza bruta de adivinación desde Linux a un dominio con Kerberos - https://github.com/TarlogicSecurity/kerbrute	190
Ilustración 59. Ejemplo de herramienta rubeus para realizar ataque de fuerza bruta de adivinación desde Windows a un dominio con Kerberos - https://github.com/Zer1t0/Rubeus	190
Ilustración 60. Pasos habituales en un ataque de kerberoasting	191
Ilustración 61. Herramienta Burp suite con utilidad en el análisis de funciones criptográficas	198
Ilustración 62. OSS-Fuzz, de Google, es un excelente ejemplo del uso de técnicas de fuzzing continuo para descubrir vulnerabilidades en el desarrollo y despliegue de software - https://github.com/google/oss-fuzz y https://github.com/google/fuzzing	211
Ilustración 63. Medir la entropía de un fichero con Radare2	218

Ilustración 64. Cálculo de la entropía de un fichero con representación visual en barras	218
Ilustración 65. Rahash2 para el cálculo de hashes, checksums y entropía (-a specify the algorithm.-b block size) https://isc.sans.edu/forums/diary/Radare2+rahash2/21577/	219
Ilustración 66. Ejemplo de extracción de claves de wifi de una red específica configurada en Windows desde consola con el comando netsh wlan show profiles name="Rajesh" key=clear	222
Ilustración 67. Ejemplo de volcado de memoria RAM para extraer las credenciales de usuario almacenadas en el fichero SAM (Windows). Las credenciales recopiladas tienen que ser crackeadas para obtenerlas en claro (https://www.andreafortuna.org/2017/11/15/how-to-retrieve-users-passwords-from-a-windows-memory-dump-using-volatility/).....	224
Ilustración 68. Esquema de esteganografía simétrica	229
Ilustración 69. Ocultación de información con la herramienta DIIT y selección de los bits a modificar en cada píxel utilizando la herramienta DIIT	233
Ilustración 70. Recuperación de información oculta con la herramienta DIIT y ataques estegoanalíticos utilizando la herramienta DIIT	233
Ilustración 71. Resultados del ataque RS utilizando la herramienta DIIT	234
Ilustración 72. Algoritmo implementado en la herramienta F5	235
Ilustración 73. Ocultación y recuperación de información utilizando la herramienta F5.....	236
Ilustración 74. Ocultación y recuperación de información con la herramienta F5 utilizando una clave secreta	236
Ilustración 75. Ejecución de Invoke-PSImage para ocultación de código malicioso en un PNG.....	237
Ilustración 76. Uso de polyglots en acciones ofensivas y defensivas.....	240

Ilustración 77. Ocultación de una imagen en el espectro de un audio con Enscribe y visualización con Baudline	241
Ilustración 78. Ocultando información con la herramienta StegoWav	242
Ilustración 79. Ocultación de información con herramienta MP3Stego...	243
Ilustración 80. Esteganografía con Hydan en programa ejecutable.....	244
Ilustración 81. Ocultación de mensaje utilizando NTFS-ADS	245
Ilustración 82. Ejecución de un código ejecutable oculto en un ADS en Windows 10.....	245
<i>Ilustración 83. Creación del fichero gato-nuevo.jpg que añade a una imagen de gato un fichero de texto al final de fichero.....</i>	<i>247</i>
Ilustración 84. Ejemplos de malware moderno que utiliza la técnica EoF para ocultar el payload malicioso.....	248
Ilustración 85. Platinum APT Group y esteganografía html.....	251
Ilustración 86. Ejemplo de uso de Covert_tcp para enviar un mensaje oculto "Hello there"	255
Ilustración 87. Ejemplo de covert-channel entre un cliente y un servidor utilizando protocolo DNS y registros TXT	257
Ilustración 88. Ejemplos de uso defensivos y ofensivos con Crypton.....	261
Ilustración 89. Ejemplo de uso de herramienta Cryptool con algoritmo Cesar	262
Ilustración 90. Interfaz web de Cyberchef.....	263
Ilustración 91. Cryptopals crypto challenges.....	265

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, meticulado, 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 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 autenticación 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 Iliada, 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 toda 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**