

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

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.....	11
Prólogo – D. Raúl Siles.....	18
Introducción - ¿Qué no es este libro?.....	23
2000 años de criptografía para profesionales perezosos.....	25
Capítulo 1. Criptografía práctica para usuarios. Protección de datos, privacidad y anonimato.....	33
Capítulo 2. Criptografía práctica para programadores y arquitectos software. Algoritmos y usos.....	37
2.1 Conceptos básicos.....	37
2.2 Criptografía simétrica	38
2.2.1 Algoritmo criptográfico simétrico AES	43
2.2.1.1 Código Python - Cifrando y descifrando con AES-CBC	44
2.2.1.2 Código Python - Cifrando y descifrando con AES-CTR	45
2.3 Criptografía asimétrica o pública.....	46
2.3.1 Algoritmo criptográfico RSA	49
2.3.1.1 ¿Cómo atacar el algoritmo RSA?	51
2.3.2 ElGamal	52
2.3.3 Curvas Elípticas	55
2.3.3.1 ¿Cómo es una curva elíptica y cómo se trabaja con ella?	56
2.3.3.2 ¿Qué curva elegir? ¿Son seguras?	59
2.3.3.3 ¿Cómo cifrar y descifrar información con curvas elípticas?	59
2.3.4 Distribución de claves.....	60
2.3.4.1 Distribución de claves criptográficas mediante curvas elípticas. El caso de ECDH	62
2.4 Funciones hash criptográficas.....	65
2.4.1 Ejemplo programación Python de funciones hash criptográficas	

.....	68
2.5 Firma digital	68
2.5.1 Firma digital con curvas elípticas ECDSA	69
2.6 MAC (Message Authentication Code)	73
2.6.1 Ejemplo de programación Python de HMAC-SHA256	75
2.7 Cifrado autenticado.....	75
2.7.1 Ejemplo de programación Python de AES256-GCM	77
2.8 Derivación de claves y password hashing	79
2.8.1 Ejemplo de derivación de clave basada en PBKDF2 con Python	81
2.8.2 Ejemplo en Python de derivación de clave Scrypt.....	84
2.8.3 Ejemplo en Python de derivación de clave basada en Argon2 ...	85
2.9 Generación segura de números aleatorios y pseudoaleatorios	86
2.9.1 Ejemplo de creación de números aleatorios en Python.....	88
2.10 Certificados digitales y codificación X509v3	89
2.10.1 ¿Cómo se usan los certificados digitales en un navegador web? ¿Cómo dificultar la suplantación?.....	93
2.11 Rellenos y padding.....	94
2.12 Computación cuántica. Circuitos cuánticos y corrección de errores cuánticos	97
2.12.1 El algoritmo de Shor y de Grover	98
2.13 Criptografía cuántica y postcuántica	101
2.13.1 ¿Qué contramedidas existen frente a un ordenador cuántico?	103
2.14 Blockchain y criptomonedas.....	106
2.14.1 ¿Cuáles son los fundamentos criptográficos más interesantes?	108
2.14.2 ¿Es posible atacar blockchain o una criptomoneda? ¿Cómo audito su seguridad? ¿Cómo puedo programar de forma segura esta tecnología?	

.....	109
2.14.3 ¿Cómo me formo? ¿Cómo empiezo?	109
2.15 Machine Learning y criptografía	111
2.16 Privacy-Enhancing Technology (PET)	113
2.16.1 Criptografía homomórfica. Computación de datos cifrados... ..	113
2.16.2 Computación multiparte segura y PSI (Private Set Intersection)	117
2.16.2.1 Criptografía umbral. Secreto compartido	119
2.16.3 Cifrado de datos con preservación de formato.....	121
2.16.4 Prueba de conocimiento cero - ZKP	122
2.16.5 Privacidad diferencial.....	123
2.17 Criptografía ligera en Internet of Things (IoT). Lightweight Cryptography	125
2.18 End-to-End (E2E) Encryption. Perfect Forward Secrecy.....	128
2.19 Criptografía y hardware. Almacenamiento seguro de claves	129
2.20 Librerías criptográficas para desarrolladores. ¿Qué algoritmo elegir?¿Cuál es el mejor diseño criptográfico?.....	131
2.20.1 Criptografía y librerías en cloud	132
2.21 Auditoría de código criptográfico. CD/CI y SDLC.....	134
2.22 Identidad digital y JSON Web Token (JWT).....	137
2.23 Criptoanálisis	141
2.23.1 Conceptos útiles para entender los ataques y la robustez criptográfica. IND-CPA, IND-CCA1 e IND-CCA2	141
2.23.2 La criptografía no se ataca, se esquiva.....	143
Capítulo 3. Criptografía aplicada para pentesters y hackers éticos.....	149
3.1 Seguridad criptográfica en las comunicaciones web. SSL/TLS y certificados digitales	150
3.1.1 Ataques criptográficos a los protocolos SSL/TLS	151

3.1.1.1 Ataques basados en compresión y tamaño de petición/respuesta.....	152
3.1.1.2 Ataques basados en implementaciones incorrectas y mal uso de algoritmo	154
3.1.1.3 Ataques basados en downgrade y flujo del protocolo	161
3.1.1.4 Ataques basados en relleno/padding.....	162
3.1.1.4.1 ¿Cómo proteger el padding de una comunicación? El caso de Lucky13	165
3.1.1.5 Ataques a TLS 1.3	168
3.1.1.6 Lecciones aprendidas en ataques criptográficos a TLS/SSL	173
3.1.2 Certificados digitales. Fuga de información y fingerprinting...	175
3.2 Cracking de contraseñas y suplantación de autenticación.....	181
3.2.1 <i>Basics</i> y recomendaciones.....	181
3.2.1.1 Atacando e identificando. Fuerza bruta, colisiones y codificación.....	182
3.2.1.2 Aplicaciones de cracking. John The Ripper y Hashcat	183
3.2.2 Creación y expansión de diccionarios de cracking de contraseñas	185
3.2.3 Credenciales en sistemas operativos. Cracking y evasión de autenticación.....	188
3.2.3.1 Sistema operativo Microsoft Windows	188
3.2.3.2 Sistema operativo Linux y MAC.....	193
3.2.4 Evasión de autenticación online y autenticación basada en contraseña.....	194
3.2.4.1 Ataque a la autenticación en protocolos basada en contraseña	194
3.2.4.2 Client-side attacks. Captchas, tokens JWT y TOTP.....	197

3.2.4.3 Burp suite y extensiones. Atacando la criptografía y bypass autenticación	199
3.2.5 Cracking de credenciales de software de cifrado y secure password storage.....	201
3.2.6 Cracking de credenciales en documentos ofimáticos y certificados digitales.....	202
3.2.7 Cracking de credenciales en comunicaciones inalámbrica	206
3.3 Fuzzing en criptografía y tecnologías blockchain. Detectando implementaciones incorrectas y vulnerabilidades	211
3.4 Herramientas para CTF (Capture the flag). Criptoanálisis y estegoanálisis	214
Capítulo 4. Criptografía para analistas.....	216
4.1 Criptografía y malware. Ransomware y cryptojacking.....	217
4.2 Forense criptográfico. Extrayendo credenciales.....	222
4.3 Esteganografía y canales encubiertos. Pentester, analistas y forenses	226
4.3.1 Esteganografía en la actualidad. Definición de conceptos.....	226
4.3.2 Clasificación de sistemas esteganográficos modernos. Portadores	228
4.3.3 Técnicas esteganográficas en la actualidad.....	231
4.3.3.1 Ocultación de información en imágenes digitales	232
4.3.3.1.1 Ocultando con Digital Invisible Ink Toolkit	232
4.3.3.1.2 Ocultación en imágenes JPEG con F5	235
4.3.3.1.3 Ocultación en imágenes PNG. El caso de Invoke-PSImage	237
4.3.3.1.4 Stegosploit, polyglots y APT-Modernos. Stegomalware en imágenes digitales	238
4.3.3.2 Ocultación de información en audio digital	241

4.3.3.3 Ocultación en sistemas de ficheros y formatos	244
4.3.3.4 Esteganografía en código interpretado. Lenguaje HTML y XML.....	250
4.3.3.5. Canales encubiertos en protocolos de comunicación. Network steganography	252
4.3.3.5.1. Canal encubierto en TCP mediante número inicial de secuencia. Ejemplo con Covert-tcp.....	255
4.3.3.5.2. Canal encubierto en DNS. Mística – La navaja suiza.	257
4.3.3.6. Herramientas de estegoanálisis. Detección práctica de información oculta con esteganografía.....	258
Capítulo 5. Formación continua en criptografía. Libros y recursos.....	261

Índice de ilustraciones

Ilustración 1. Clasificación de los métodos clásicos de cifra y algunos ejemplos.....	26
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.....	28
Ilustración 3. Web oficial proyecto PRISM Break.....	35
Ilustración 4. Esquema de cifrado simétrico	39
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).....	39
Ilustración 6. Cifrado y descifrado con modo CBC y CTR.....	41
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	41
Ilustración 8. Modo de cifrado GCM.....	42
Ilustración 9. Estructura del algoritmo criptográfico AES.....	44
Ilustración 10. Generación de claves RSA con el software educativo genRSA	50
Ilustración 11. Ejemplo de expresiones analíticas para suma de dos puntos en una curva. $P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3)$	57
Ilustración 12. Ejemplo de expresiones analíticas para multiplicación de un punto $R(x, y)$	58
Ilustración 13. Visualización de los puntos de una curva elíptica	59

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>..... 61

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> 64

Ilustración 16. Cálculo en Python del hash criptográfico SHA-256, SHA3-256, BLAKE2s y RIPEMD-160 68

Ilustración 17. Creación y validación de MAC..... 73

Ilustración 18. Cifrado autenticado - https://en.wikipedia.org/wiki/Authenticated_encryption..... 74

Ilustración 19. Ejemplo de uso de la herramienta CyberChef del GCHQ para calcular un HMAC-SHA256 75

Ilustración 20. Modo de cifrado autenticado AES-GCM..... 76

Ilustración 21. Ejemplo de programación en Python de AES-GCM 78

Ilustración 22. Recommendation for Password-Based Key Derivation Part 1: Storage Applications. NIST. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132> 81

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.....	82
Ilustración 24. Ejemplo de uso de la herramienta CyberChef del GCHQ para cálculo de PBKDF2.....	83
<i>Ilustración 25. Programación en Python de KDF script y ejemplo de análisis de duración de tiempo</i>	<i>85</i>
Ilustración 26. Estructura de un certificado X.509v3	90
Ilustración 27. Ejemplo de certificado X.509 y como se puede ver en un navegador web.....	92
Ilustración 28. Generación de certificado auto firmado con OpenSSL	92
Ilustración 29. Validación de la fecha de expiración de un certificado digital desde consola con OpenSSL	92
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)	95
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-	96
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).....	100
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-Gagliardoni-Quantum-Security-And-Cryptography-Youre-Probably-Doing-It-Wrong.pdf	105
<i>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.....</i>	107
Ilustración 36. Comparación de algunos de los esquemas SWHE más famosos.....	115
Ilustración 37. Operaciones permitidas en librerías y algoritmos criptográficos con uso homomórfico	116
Ilustración 38. Ejemplos de algoritmos criptográficos ligeros recogidos en la literatura.....	127
Ilustración 39. Métricas habituales analizadas para el diseño o uso de algoritmos criptográficos ligeros.....	127
Ilustración 41. Funcionamiento de los elementos de XACML - https://es.wikipedia.org/wiki/XACML	139
Ilustración 42. Funcionamiento de SAML.....	139
Ilustración 43. El protocolo TLS en realidad se compone de diversos protocolos que ayudarán en la protección de la información	151
Ilustración 44. Ejemplo de inyección de código JavaScript en el ataque Sweet32	156
Ilustración 45. Cifrado de bloque en modo CBC.....	158
Ilustración 46. Esquema visual del ataque BEAST	159
Ilustración 47. Ejemplo de adivinación de cookies con BEAST	160
Ilustración 48. Ejemplos de codificación de padding al final de una información	162
Ilustración 49. Bleichenbacher padding oracle attack	164
Ilustración 50. Esquemas de cifrado autenticado.....	166

Ilustración 51. Proceso de cifrado (DTLS)	167
Ilustración 52. Esquema general de ataque 9 lives of Bleichenbachers cat	170
Ilustración 53. Proceso completo de ataque a TLS 1.3 con 9 lives	171
Ilustración 54. Resumen de ataques de padding a implementación TLS/SSL modernas	172
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	174
Ilustración 56. Herramienta para intentar deducir del tamaño de una información con qué algoritmo fue protegida - https://tools.kali.org/password-attacks/hash-identifier	182
Ilustración 57. Ejemplos de uso de Crackmapexec para conexión remota a equipos.....	190
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	191
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	191
Ilustración 60. Pasos habituales en un ataque de kerberoasting	192
Ilustración 61. Herramienta Burp suite con utilidad en el análisis de funciones criptográficas	199
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	212
Ilustración 63. Medir la entropía de un fichero con Radare2	219

Ilustración 64. Cálculo de la entropía de un fichero con representación visual en barras	219
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/	220
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	223
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/).....	225
Ilustración 68. Esquema de esteganografía simétrica	230
Ilustración 69. Ocultación de información con la herramienta DIIT y selección de los bits a modificar en cada píxel utilizando la herramienta DIIT	234
Ilustración 70. Recuperación de información oculta con la herramienta DIIT y ataques estegoanalíticos utilizando la herramienta DIIT	234
Ilustración 71. Resultados del ataque RS utilizando la herramienta DIIT	235
Ilustración 72. Algoritmo implementado en la herramienta F5	236
Ilustración 73. Ocultación y recuperación de información utilizando la herramienta F5.....	237
Ilustración 74. Ocultación y recuperación de información con la herramienta F5 utilizando una clave secreta	237
Ilustración 75. Ejecución de Invoke-PSImage para ocultación de código malicioso en un PNG.....	238
Ilustración 76. Uso de polyglots en acciones ofensivas y defensivas.....	241

Ilustración 77. Ocultación de una imagen en el espectro de un audio con Enscribe y visualización con Baudline	242
Ilustración 78. Ocultando información con la herramienta StegoWav	243
Ilustración 79. Ocultación de información con herramienta MP3Stego...	244
Ilustración 80. Esteganografía con Hydan en programa ejecutable.....	245
Ilustración 81. Ocultación de mensaje utilizando NTFS-ADS	246
Ilustración 82. Ejecución de un código ejecutable oculto en un ADS en Windows 10.....	246
<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>248</i>
Ilustración 84. Ejemplos de malware moderno que utiliza la técnica EoF para ocultar el payload malicioso.....	249
Ilustración 85. Platinum APT Group y esteganografía html.....	252
Ilustración 86. Ejemplo de uso de Covert_tcp para enviar un mensaje oculto "Hello there"	256
Ilustración 87. Ejemplo de covert-channel entre un cliente y un servidor utilizando protocolo DNS y registros TXT	258
Ilustración 88. Ejemplos de uso defensivos y ofensivos con Crypton.....	262
Ilustración 89. Ejemplo de uso de herramienta Cryptool con algoritmo Cesar	263
Ilustración 90. Interfaz web de Cyberchef.....	264
Ilustración 91. Cryptopals crypto challenges.....	266

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, metódico, 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**

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 criptología¹. 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 estadística³ 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 criptoanalistas⁴, 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 (monográfica a poligráfica) 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 contruidos 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.

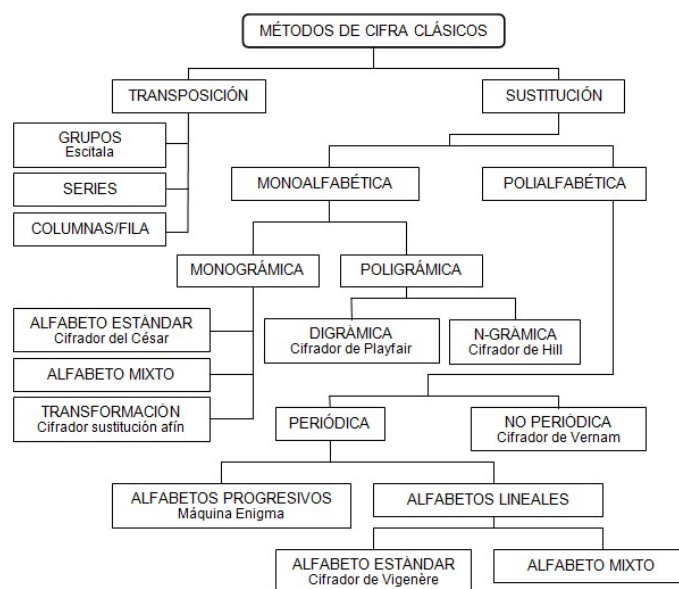


Ilustración 1. Clasificación de los métodos clásicos de cifra y algunos ejemplos

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 cifrado⁵⁻⁶, 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_\(m%C3%A1quina\)](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 difusión⁷ y confusión⁸ 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 criptografía⁹ 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 actuales¹⁰.

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 maestra¹¹.

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 avalancha¹². 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-linealidad¹⁴ y **estructuras específicas para mezclar las operaciones anteriores**. Un ejemplo famoso de esto es la red o estructura tipo Feistel¹⁵. 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.

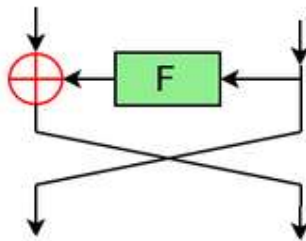


Ilustración 2. La red Feistel coge un bloque de N bits y lo trocea en dos partes. La parte derecha sale como la nueva parte izquierda y la nueva parte derecha será el resultado de hacer una operación or-exclusiva de la entrada izquierda con una serie de modificaciones, función F, de la entrada derecha. 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 las 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 vueltas¹⁶¹⁷ 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 Vernam¹⁸ y el esquema OTP, la única propuesta criptográfica teóricamente irrompible. Recuérdese que el problema práctico del cifrado de Vernam es la distribución de la clave¹⁹⁻²⁰.

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 confianza²¹ (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 Zimmermann²² 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 época²³⁻²⁴, 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 interceptadas²⁵ de manera subrepticia.
- *Criptografía postcuántica.* Diseño de nuevos algoritmos criptográficos resistentes frente a la futura computación cuántica²⁶.
- *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 partes²⁷.
- *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 imaginable el poder de las matemáticas y la algoritmia puede sobreponerse a cualquier dificultad²⁹. O al menos, así es en teoría.

La criptografía³⁰, al menos desde un punto de vista práctico, no se “ataca” se esquivo. 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.

Capítulo 5. Formación continua en criptografía. Libros y recursos

La educación es el pasaporte hacia el futuro,
el mañana pertenece a aquellos que
se preparan para él en el día de hoy.

Malcolm X

La formación en criptografía se puede apoyar en múltiples fuentes en soporte variados. A continuación, se van a citar algunas herramientas y sitios de referencia para incrementar o validar su conocimiento en esta disciplina.

- **Crypton** (<https://github.com/ashutosh1206/Crypton>)

*Crypton is an educational library to **learn** and **practice** Offensive and Defensive Cryptography. It is basically a collection of explanation and implementation of all the existing vulnerabilities and attacks on various Encryption Systems (Symmetric and Asymmetric), Digital Signatures, Message Authentication Codes and Authenticated Encryption Systems. Each attack is also supplemented with example challenges from "Capture The Flag" contests and their respective write-ups. Individuals who are already acquainted (or are into CTFs) with this field can use Crypton as a tool to solve challenges based on a particular existing vulnerability.*

1. Block Ciphers

S.N o.	Topic	Explanat ion	Impl./Exp loit	Challen ge#
1	Block Cipher Basics- working of block ciphers, padding etc.	[link]		
2	Modes of Encryption- different modes of operation on block ciphers: ECB, CBC, CTR	[link]		
3	Block Size Detection- detect blocksize of a block cipher encrypting data on a remote service	[link]		
4	Mode Detection- detect type of mode of encryption: independent or dependent encryption of blocks	[link]		
5	ECB Byte at a Time- byte at a time decryption of a <code>secret</code> string running on a remote service encrypting <code>input + secret</code> in ECB mode	[link]		[link]
6	CBC IV Detection- detect the value of Initialisation Vector on a remote service that is encrypting our input using a block cipher in CBC mode	[link]	[link]	
7	CBC Bit Flipping Attack- exploiting cookie generation mechanism to login as admin when cookie is generated using a block cipher in CBC mode	[link]		[link]
8	CBC Byte at a Time- byte at a time decryption of a <code>secret</code> string running on a remote service encrypting <code>input + secret</code> in ECB mode	[link]	[link]	
9	CBC Padding Oracle Attack- decryption of data encrypted by a <code>vulnerable</code> service providing encryption/decryption	[link]		[link]
10	CTR Bit Flipping- exploiting cookie generation mechanism to login as admin when cookie is generated using a block cipher in CBC mode	[link]		[link]

2. RSA Encryption

S.No.	Topic	Explanation	Impl./Exploit	Challenge#
1	Unpadded RSA Enc/Dec - key generation, distribution, encryption/decryption, verification of decryption formula and padding in RSA	[link]		
2	Direct Root Attack - attack on unpadded RSA with low public key exponent	[link]		
3	Fermat's Factorisation - technique used to factor modulus n when p and q values are in proximity	[link]	[link]	[link]
4	Pollard's p-1 Factorisation - technique to factorise n when both of its factors p & q , $p-1$ and $q-1$ have very small prime divisors	[link]	[link]	[link]
5	Common Modulus Attack - decrypt ciphertext when it's corresponding plaintext is encrypted two different times with the same modulus n	[link]	[link]	[link]
6	Common Prime Attack - retrieve factors of moduli n_1 and n_2 when they have a common factor	[link]		[link]
7	Wiener's Attack - get value of decryption key exponent d when $d < N^{0.25}$	[link]	[link]	[link]
8	Wiener's Attack Variant - get value of decryption key exponent d when d is a few bits greater than $N^{0.25}$ or $d < N^{0.25}$	[link]	[link]	[link]
9	Coppersmith's Attack - coppersmith's theorem, attack on stereotyped messages and factoring n with high bits known	[link]	[link]	[link]
10	Franklin Reiter Related Message Attack - attack to retrieve related messages encrypted using the same modulus	[link]	[link]	[link]
11	Hastad's Broadcast Attack- with extension - attack to retrieve a message broadcasted among different people, encrypted using same exponent but different moduli	[link]	[link] - script needs to be fixed	[link]
12	PKCS1-v1.5-Padded-RSA-Encryption/Decryption - ASN1 encoding, padded RSA encryption (needs to be fixed)			
13	Intro-RSA-Challenges - basic challenges in RSA related to Number Theory	[link]		[link]

3. Message Authentication Codes (MACs)

S.No.	Topic	Explanation	Impl./Exploit	Challenge#
1	Message Authentication Code - internals and security analysis of MACs	[link]		
2	CBC MAC Forgery - generating two message M_1 and M_2 having the same CBC-MAC authentication tag	[link]		[link]
3	Length Extension Attack on CBC-MAC - generate a valid authentication tag of message $M_1 M_2$ (concatenation) given MAC(M_1)	[link]	[link]	

Ilustración 86. Ejemplos de uso defensivos y ofensivos con Crypton

- **Cryptool**⁸¹³ (<https://www.cryptool.org/en/ct1-downloads>)

*Es un software libre que ilustra conceptos criptográficos. Es el programa de aprendizaje electrónico de uso más extendido en el mundo en el área de la criptología. Con más de 60 algoritmos y de herramientas para el análisis. La interfaz gráfica y la abundante información en línea permiten al usuario, incluso a un novato en Internet, introducirse en los misterios de la criptografía. Los mecanismos más clásicos, así como la criptografía asimétrica RSA, la criptografía basada en curvas elípticas, firmas digitales o el protocolo de intercambio de claves Diffie-Hellman, se explican utilizando animaciones. También contiene un tutorial sobre primos y teoría de números elemental*⁸¹⁴.

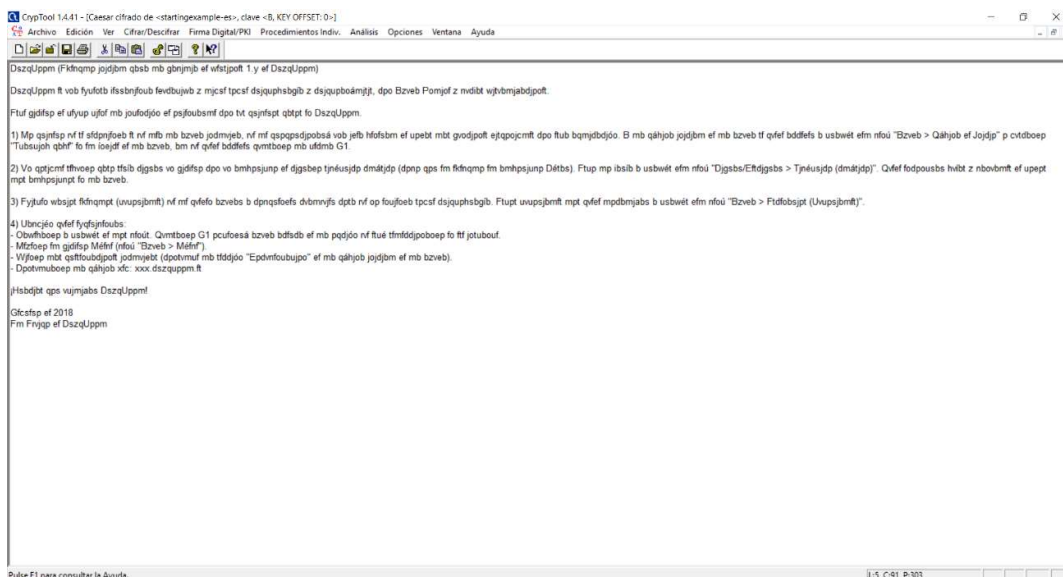


Ilustración 87. Ejemplo de uso de herramienta Cryptool con algoritmo Cesar

⁸¹³ <https://www.cryptool.org/images/ct1/presentations/CrypTool1-Presentation-en.pdf>

⁸¹⁴ <https://es.wikipedia.org/wiki/Cryptool>

- **CyberChef** - The Cyber Swiss Army Knife. A web app for encryption, encoding, compression and data analysis) - <https://gchq.github.io/CyberChef/>

A simple, intuitive web app for analysing and decoding data without having to deal with complex tools or programming languages. CyberChef encourages both technical and non-technical people to explore data formats, encryption and compression.

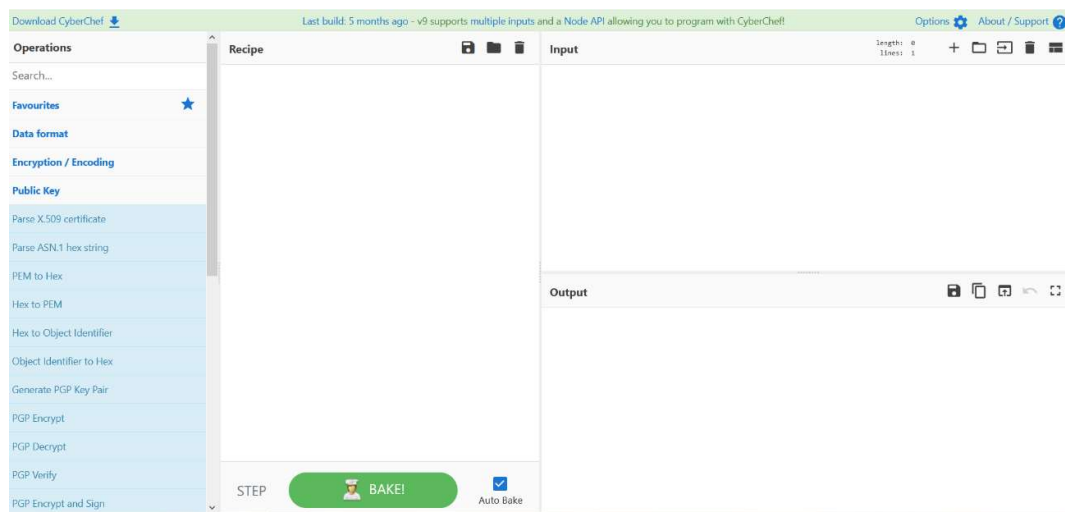


Ilustración 88. Interfaz web de Cyberchef

- **CryptoVenom** – The Cryptography Swiss Army Knife (<https://github.com/lockedbyte/cryptovenom>)

CryptoVenom is an OpenSource tool which contains a lot of cryptosystems and cryptoanalysis methods all in one, including classical algorithms, hash algorithms, encoding algorithms, logic gates, mathematical functions, modern symmetric and asymmetric encryptions etc.

- **Certificación de criptografía CriptoCert Certified Crypto Analyst** – <https://www.cryptocert.com>

- **Red temática de criptografía y seguridad de la información Criptored**⁸¹⁵

Es la red temática de mayor difusión de conocimiento en criptografía en lengua española durante los últimos 22 años. Sus proyectos han permitido distribuir documentos e información audiovisual gratuita a varios millones de usuarios en todo el planeta. Algunos de los proyectos más famosos a consultar son: Intypedia⁸¹⁶, Crypt4you⁸¹⁷, Thoth⁸¹⁸ o Crypt4class⁸¹⁹.

- **Crypto challenges** - Cryptopals (<https://cryptopals.com/>), Matasano-cryptopals (<https://github.com/JesseEmond/matasano-cryptopals>), HackTheBox Challenge Crypto⁸²⁰ (<http://homepages.rpi.edu/~wangy52/PersonalWebsite/build/html/Cybersecurity%20Labs/HTB-Crypto.html>), Crypto-CTFs (<https://github.com/mindcrypt/Cryptanalysis>), CryptoHack (<https://cryptohack.org/>), MTC3 (<https://www.mysterytwisterc3.org/en/>).

⁸¹⁵ <http://www.criptored.upm.es/paginas/presentacion.html>

⁸¹⁶ <http://www.criptored.upm.es/intypedia/>

⁸¹⁷ <http://www.criptored.upm.es/crypt4you/portada.html>

⁸¹⁸ <http://www.criptored.upm.es/thoth/>

⁸¹⁹ <https://www.youtube.com/channel/UC5t0X0VGOT2P8sj7gXPeHIg>

⁸²⁰ Existen multitud de plataformas de entrenamiento de habilidades de *hacking* donde podrá encontrar retos de criptografía. Algún ejemplo: <https://www.vulnhub.com>, <https://practicalpentestlabs.com>, <https://www.amanhardikar.com/mindmaps/Practice.html>, etc.

the cryptopals crypto challenges

Set 1: Basics
Set 2: Block crypto
Set 3: Block & stream crypto
Set 4: Stream crypto and randomness
Set 5: Diffie-Hellman and friends
Set 6: RSA and DSA
Set 7: Hashes
Set 8: Abstract Algebra

Welcome to the challenges

Work in progress.

This site will host all eight sets of our crypto challenges, with solutions in most mainstream languages.

But: it doesn't yet. If we waited to hit "publish" until everything was here, we might be writing this in 2015. So we're publishing as we go. In particular: give us a little time on the challenge solutions.

We can't introduce these any better than [Maciej Ceglowski](#) did, so read that blog post first.

We've built a collection of 48 exercises that demonstrate attacks on real-world crypto.

This is a different way to learn about crypto than taking a class or reading a book. We give you problems to solve. They're derived from weaknesses in real-world systems and modern cryptographic constructions. We give you enough info to learn about the underlying crypto concepts yourself. When you're finished, you'll not only have learned a good deal about how cryptosystems are built, but you'll also understand how they're attacked.

What Are The Rules?

There aren't any! For several years, we ran these challenges over email, and asked participants not to share their results. *The honor system worked beautifully!* But now we're ready to set aside the ceremony and just publish the challenges for everyone to work on.

How Much Math Do I Need To Know?

If you have any trouble with the math in these problems, you should be able to find a local 9th grader to help you out. It turns out that many modern crypto attacks don't involve much hard math.

How Much Crypto Do I Need To Know?

None. That's the point.

Ilustración 89. Cryptopals crypto challenges

- **Libros y recursos online.** Con un poco de curiosidad encontrará multitud de referencias en esta disciplina. En este punto le recomiendo algunas referencias para empezar basadas en mi experiencia. La mayoría son gratuitas.

- *100 Best Cryptography Books of All Time.*

<https://bookauthority.org/books/best-cryptography-books>

- *Practical Cryptography for Developers.* <https://cryptobook.nakov.com/>

- *Seguridad en el protocolo SSL-TLS. Ataques criptoanalíticos modernos.*

https://github.com/mindcrypt/libros/blob/master/Book_Seguridad_en_el_protocolo_SSL-TLS_Atques_criptoanaliticos_modernos_Dr._Alfonso_Muoz_-_27092020.pdf

- *Libro Electrónico de Seguridad Informática y Criptografía.* Jorge Ramío

- http://www.criptored.upm.es/guiateoria/gt_m001s1.htm

- *Criptografía y Seguridad en Computadores.* Manuel Lucena.

<http://criptografiayseguridad.blogspot.com/p/criptografia-y-seguridad-en.html>

- Criptografía Digital. Fundamentos y aplicaciones. Jose Pastor et al. - <https://www.casadellibro.com/libro-criptografia-digital-fundamentos-y-aplicaciones/9788477334910/596107>
- *Handbook of Applied Cryptography*. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone - <http://cacr.uwaterloo.ca/hac/>
- Applied Cryptography. Protocols, Algorithms, and Source Code in C - <https://www.schneier.com/books/applied-cryptography/>
- Serious Cryptography. A practical Introduction to Modern Encryption - <https://nostarch.com/seriouscrypto>
- Coursera Crypto (Dan Boneh) <https://www.coursera.org/learn/crypto>
- Criptografía en el mundo real. Aplicaciones sorprendentes de la criptografía para desafíos del día a día (Gonzalo Álvarez Marañón) - <https://cmr.e-paths.com/>
- Crypto 101 - <https://www.crypto101.io/>
- *Encyclopedia of Theoretical and Applied Cryptography (Foundations of Cryptography and Applications of Cryptography (Cryptographic Protocols)* - http://cryptowiki.net/index.php?title=Main_Page
- Real Word cryptography - <https://soatok.blog/>
- Blog de Thai Duong - <https://vnhacker.blogspot.com/>
- David Wong - <https://www.cryptologie.net/>
- Matthew Green - <https://blog.cryptographyengineering.com/>
- <https://cryptovillage.org>
- <https://passwordvillage.org>