

# ÍNDICE

---

<b>PRÓLOGO</b> .....	<b>27</b>
<b>CAPÍTULO 1. INTRODUCCIÓN A LA CRIPTOGRAFÍA</b> ..	<b>29</b>
1.1. IDEAS BÁSICAS Y CONCEPTOS GENERALES . . . . .	29
1.2. SUSTITUCIÓN Y TRANSPOSICIÓN . . . . .	32
1.3. MÉTODOS CRIPTOGRÁFICOS Y SEGURIDAD . . . . .	35
1.3.1. Clasificación de ataques criptoanalíticos . . . . .	36
1.3.2. Condiciones de secreto perfecto . . . . .	38
1.4. DISPOSITIVOS CRIPTOGRÁFICOS . . . . .	40
1.5. CRIPTOGRAFÍA DE USO COTIDIANO . . . . .	43
<b>CAPÍTULO 2. CIFRADO EN FLUJO</b> .....	<b>45</b>
2.1. ANTECEDENTES DEL CIFRADO EN FLUJO . . . . .	45
2.2. ASPECTOS GENERALES DEL CIFRADO EN FLUJO . . . . .	47
2.3. CARACTERÍSTICAS FUNDAMENTALES DE LAS SECUENCIAS CIFRANTES . . . . .	50
2.3.1. Período . . . . .	50
2.3.2. Distribución de bits . . . . .	50
2.3.3. Imprevisibilidad . . . . .	52

2.3.4.	Test de aleatoriedad: NIST, Diehard y Tuftest . . . . .	52
2.3.5.	Seguridad de las secuencias cifrantes . . . . .	53
2.4.	GENERADORES DE SECUENCIAS CIFRANTES . . . . .	54
2.4.1.	Registros de desplazamiento realimentados linealmente	54
2.5.	APLICACIONES DEL CIFRADO EN FLUJO . . . . .	57
2.5.1.	Generadores A5 en telefonía móvil GSM y su seguridad	57
2.5.2.	Generador E0 en Bluetooth y su seguridad . . . . .	61
2.5.3.	Generador RC4 en WEP y su seguridad . . . . .	62
2.6.	HACIA UN ESTÁNDAR DE CIFRADO EN FLUJO: THE eSTREAM PROJECT . . . . .	63
2.6.1.	Características del eSTREAM Project . . . . .	64
2.6.2.	Generador Sosemanuk (perfil software): seguridad e implementación . . . . .	66
2.6.3.	Generador Trivium (perfil hardware): seguridad e implementación . . . . .	71
2.7.	EL FUTURO DEL CIFRADO EN FLUJO . . . . .	74
<b>CAPÍTULO 3. CIFRADO EN BLOQUE . . . . .</b>		<b>77</b>
3.1.	INTRODUCCIÓN . . . . .	77
3.1.1.	Propiedades del cifrado en bloque . . . . .	78
3.1.2.	Arquitectura del cifrado en bloque . . . . .	79
3.1.3.	Cifrados de Feistel . . . . .	80
3.2.	DES Y DEA . . . . .	82
3.2.1.	Estructura del DEA . . . . .	83
3.2.2.	Descifrado e involución en el DEA . . . . .	85
3.2.3.	Estructura del DEA: función $F$ . . . . .	86
3.2.4.	Expansión de claves en el DEA . . . . .	89
3.2.5.	Propiedad de complementación del DEA . . . . .	90
3.2.6.	Claves débiles y semidébiles del DEA . . . . .	90
3.2.7.	Seguridad del DEA . . . . .	91
3.2.8.	Criptografía diferencial del DEA . . . . .	91
3.2.9.	Criptografía lineal . . . . .	98

3.2.10. Rotura del DEA por prueba exhaustiva de claves . . . . .	99
3.3. CIFRADO MÚLTIPLE . . . . .	100
3.3.1. Ataque a los cifrados múltiples por encuentro a medio camino . . . . .	101
3.4. TRIPLE DEA: TDEA . . . . .	102
3.4.1. Estructura del TDEA . . . . .	102
3.5. AES Y RIJNDAEL . . . . .	103
3.5.1. Estructura del AES . . . . .	105
3.5.2. Transformación <code>SubBytes</code> . . . . .	106
3.5.3. Transformación <code>ShiftRows</code> . . . . .	108
3.5.4. Transformación <code>MixColumns</code> . . . . .	109
3.5.5. Transformación <code>AddRoundKey</code> . . . . .	109
3.5.6. Esquema de clave en el AES . . . . .	110
<b>CAPÍTULO 4. MODOS DEL CIFRADO EN BLOQUE . . . . .</b>	<b>113</b>
4.1. INTRODUCCIÓN . . . . .	113
4.2. LIBRO ELECTRÓNICO DE CÓDIGOS: ECB . . . . .	114
4.3. ENCADENAMIENTO DE BLOQUES CIFRADOS: CBC . . . . .	116
4.4. REALIMENTACIÓN DEL TEXTO CIFRADO: CFB . . . . .	119
4.5. REALIMENTACIÓN DE LA SALIDA: OFB . . . . .	121
4.6. CONTADOR: CTR . . . . .	122
4.7. CÓDIGO DE AUTENTICACIÓN DE MENSAJE: CMAC . . . . .	124
4.8. AUTENTICACIÓN Y CONFIDENCIALIDAD: CCM . . . . .	125
4.9. CONTADOR DE GALOIS: GCM-GMAC . . . . .	126
4.10. CONFIDENCIALIDAD DEL AES EN MEDIOS DE ALMACENAMIENTO: XTS-AES . . . . .	129
<b>CAPÍTULO 5. NÚMEROS ALEATORIOS . . . . .</b>	<b>133</b>
5.1. INTRODUCCIÓN . . . . .	133

5.2.	GENERACIÓN DE NÚMEROS REALMENTE ALEATORIOS	134
5.2.1.	Técnicas para eliminar el sesgo y la correlación . . . .	136
5.2.2.	Algunos generadores prácticos genuinamente aleatorios	136
5.3.	GENERACIÓN DE NÚMEROS PSEUDOALEATORIOS . . . .	137
5.3.1.	Aleatoriedad y batería de pruebas . . . . .	138
5.3.2.	PRNG criptográficamente seguros . . . . .	148
5.4.	PERMUTACIONES ALEATORIAS . . . . .	154
5.5.	NOTAS PARA EL DISEÑO DE GENERADORES . . . . .	157
<b>CAPÍTULO 6. FUNCIONES RESUMEN . . . . .</b>		<b>159</b>
6.1.	FUNCIONES RESUMEN . . . . .	159
6.2.	SEGURIDAD . . . . .	161
6.3.	FUNCIÓN MD5 . . . . .	162
6.4.	FUNCIONES SHA-0 y SHA-1 . . . . .	163
6.5.	FUNCIONES DE LA SERIE SHA-2 . . . . .	164
6.6.	FUNCIÓN SHA-3 . . . . .	165
6.7.	FUNCIONES HMAC . . . . .	166
6.8.	OTRAS FUNCIONES RESUMEN . . . . .	167
6.8.1.	Función RIPEMD-160 . . . . .	168
6.8.2.	Función Panama . . . . .	168
6.8.3.	Función Tiger . . . . .	168
6.8.4.	Función CRC32 . . . . .	168
6.9.	APLICACIONES DE LAS FUNCIONES RESUMEN . . . . .	168
6.9.1.	Firmas digitales . . . . .	169
6.9.2.	Certificados digitales . . . . .	169
6.9.3.	DNIE . . . . .	169
6.9.4.	Integridad de datos . . . . .	169
6.9.5.	Repositorios de datos . . . . .	169
6.9.6.	Detección de software dañino . . . . .	170

**CAPÍTULO 7. CIFRADO CON TEORÍA DE NÚMEROS ... 171**

7.1. ACUERDO DE CLAVE DE DIFFIE-HELLMAN . . . . .	171
7.1.1. Seguridad . . . . .	172
7.2. CRIPTOSISTEMAS ASIMÉTRICOS . . . . .	174
7.2.1. Definiciones . . . . .	174
7.2.2. Protocolo de envoltura digital y criptosistema híbrido	176
7.3. CRIPTOSISTEMA RSA . . . . .	178
7.3.1. Generación de claves . . . . .	179
7.3.2. Cifrado de mensajes . . . . .	179
7.3.3. Descifrado de mensajes . . . . .	180
7.3.4. Generación de claves y descifrado con RSA-CRT . . .	180
7.3.5. Seguridad . . . . .	181
7.4. CRIPTOSISTEMA DE ELGAMAL . . . . .	187
7.4.1. Generación de claves . . . . .	188
7.4.2. Cifrado de mensajes . . . . .	189
7.4.3. Descifrado de mensajes . . . . .	189
7.4.4. Seguridad . . . . .	190
7.5. OTROS CRIPTOSISTEMAS . . . . .	190
7.5.1. De Rabin . . . . .	191
7.5.2. De mochila . . . . .	194

**CAPÍTULO 8. CIFRADO CON CURVAS ALGEBRAICAS . 199**

8.1. CRIPTOSISTEMA DE CURVAS ELÍPTICAS . . . . .	199
8.1.1. Curvas elípticas definidas sobre cuerpos . . . . .	200
8.1.2. El grupo de puntos de una curva elíptica . . . . .	202
8.2. ACUERDO DE CLAVE CON CURVAS ELÍPTICAS . . . . .	205
8.2.1. Acuerdo de clave de Diffie-Hellman con curvas elípticas: ECDH . . . . .	205
8.2.2. Acuerdo de clave de Menezes-Qu-Vanstone con curvas elípticas: ECMQV . . . . .	208

8.3.	CRIPTO SISTEMAS DE CURVAS ELÍPTICAS: ECC . . . . .	209
8.3.1.	Criptosistema ElGamal para curvas elípticas . . . . .	211
8.3.2.	Criptosistema Menezes-Vanstone para curvas elípticas . . . . .	212
8.3.3.	Criptosistema ECIES . . . . .	213
8.3.4.	Seguridad . . . . .	216
8.4.	CRIPTO SISTEMA DE CURVAS HIPERELÍPTICAS . . . . .	216
<b>CAPÍTULO 9. FIRMAS DIGITALES . . . . .</b>		<b>221</b>
9.1.	ESQUEMAS DE FIRMA DIGITAL . . . . .	221
9.1.1.	Esquema de firma para un mensaje público . . . . .	224
9.1.2.	Esquema de firma para un mensaje secreto . . . . .	225
9.1.3.	Falsificación existencial de una firma . . . . .	227
9.2.	FIRMA DIGITAL RSA . . . . .	228
9.2.1.	Firma digital para RSA . . . . .	228
9.2.2.	Firma digital para RSA-CRT . . . . .	228
9.2.3.	Seguridad . . . . .	229
9.3.	FIRMA DIGITAL ELGAMAL . . . . .	230
9.3.1.	Firma digital para ElGamal . . . . .	231
9.3.2.	Seguridad . . . . .	232
9.4.	FIRMA DIGITAL DEL NIST: DSA . . . . .	235
9.4.1.	Norma de firma digital: DSS . . . . .	235
9.4.2.	Algoritmo de firma DSA . . . . .	236
9.4.3.	Seguridad . . . . .	236
9.5.	FIRMA DIGITAL CON CURVA ELÍPTICA: ECDSA . . . . .	238
9.5.1.	Algoritmo estándar de firma ECDSA . . . . .	239
9.5.2.	Seguridad . . . . .	239
9.6.	OTRAS FIRMAS DIGITALES . . . . .	239
9.6.1.	Firma de Rabin . . . . .	240
9.6.2.	Firma de Fiat-Shamir . . . . .	241
9.6.3.	Firma de Schnorr . . . . .	241
9.6.4.	Firma con curvas hiperelípticas: HECDSA . . . . .	243

9.6.5. Firmas con funcionalidades adicionales . . . . .	243
<b>CAPÍTULO 10. USOS ACTUALES DE LA CRIPTOGRAFÍA</b>	<b>249</b>
10.1. CERTIFICADOS DIGITALES . . . . .	249
10.2. DNIE . . . . .	253
10.2.1. Soporte físico . . . . .	253
10.2.2. Soporte lógico . . . . .	257
10.2.3. Expedición de un DNIE . . . . .	258
10.2.4. Usos del DNIE . . . . .	260
10.2.5. Líneas de caracteres OCR-B y dígitos de control del DNIE . . . . .	263
10.3. PASAPORTE ELECTRÓNICO . . . . .	267
10.3.1. Control de acceso básico: BAC . . . . .	269
10.3.2. Control de acceso extendido: EAC . . . . .	270
10.4. OTROS PROTOCOLOS Y APLICACIONES . . . . .	271
10.4.1. Identificación amigo/enemigo . . . . .	271
10.4.2. Lanzamiento de una moneda por teléfono . . . . .	272
10.4.3. Póquer por teléfono . . . . .	272
10.4.4. Descubrimiento parcial de secretos . . . . .	273
10.4.5. Venta e intercambio de secretos . . . . .	273
10.4.6. Transferencia inconsciente . . . . .	274
10.4.7. Descubrimiento mínimo y nulo . . . . .	274
10.4.8. Reparto de secretos . . . . .	274
10.4.9. Criptografía visual . . . . .	275
10.4.10. Canales subliminales . . . . .	276
10.4.11. Esquema electoral . . . . .	277
10.4.12. Computación con datos cifrados . . . . .	277
10.4.13. Protección de software y hardware . . . . .	277
<b>CAPÍTULO 11. ATAQUES A LA IMPLEMENTACIÓN</b> . . . . .	<b>279</b>
11.1. INTRODUCCIÓN . . . . .	279

---

11.2. ATAQUES POR ANÁLISIS TEMPORAL . . . . .	281
11.2.1. Ataques por análisis de la caché . . . . .	283
11.2.2. Ataques por análisis de la predicción de saltos . . . . .	283
11.3. ATAQUES POR ANÁLISIS DE POTENCIA . . . . .	283
11.3.1. Modelos de fuga . . . . .	284
11.3.2. Análisis simple . . . . .	285
11.3.3. Análisis diferencial . . . . .	286
11.3.4. Ataques por correlación . . . . .	288
11.3.5. Ataques con plantilla . . . . .	290
11.3.6. Análisis diferencial de orden superior . . . . .	290
11.4. ATAQUES POR ANÁLISIS DE EMANACIONES ELECTROMAGNÉTICAS . . . . .	291
11.4.1. Ataques específicos a dispositivos RFID . . . . .	292
11.5. ATAQUES POR INDUCCIÓN DE FALLOS . . . . .	293
11.5.1. Técnicas de inducción de fallos . . . . .	293
11.5.2. Tipos de fallos . . . . .	295
11.5.3. Modelos de fallos . . . . .	296
11.5.4. Ataque por inducción de fallos contra el RSA . . . . .	298
11.5.5. Análisis diferencial de fallos contra el DEA . . . . .	299
11.6. ATAQUES UTILIZANDO MÉTODOS COMBINADOS . . . . .	300
11.7. CONTRAMEDIDAS . . . . .	301
11.7.1. Protección contra los ataques por canales laterales . . . . .	302
11.7.2. Protección contra los ataques por inducción de fallos . . . . .	308
<b>REFERENCIAS . . . . .</b>	<b>313</b>
<b>GLOSARIO DE TÉRMINOS . . . . .</b>	<b>349</b>
<b>ÍNDICE ALFABÉTICO . . . . .</b>	<b>357</b>



## LISTA DE FIGURAS

---

1.1.	Proceso general de cifrado y descifrado . . . . .	30
1.2.	Clasificación general de criptosistemas . . . . .	33
1.3.	Fotografía de un chip criptográfico . . . . .	41
1.4.	Chip y antena insertados en la solapa de un pasaporte electrónico	42
2.1.	Procedimiento de cifrado en flujo . . . . .	49
2.2.	Registro de desplazamiento realimentado linealmente (LFSR)	55
2.3.	Esquema general del generador A5/1 . . . . .	58
2.4.	Esquema general del generador A5/2 . . . . .	59
2.5.	Esquema general del generador $E0$ . . . . .	61
2.6.	Esquema general del sistema de cifrado en WEP . . . . .	62
2.7.	LFSR utilizado en Sosemanuk . . . . .	68
2.8.	Esquema general del generador Sosemanuk . . . . .	70
2.9.	Esquema general del generador Trivium . . . . .	73
3.1.	Redes de Feistel para cifrado (izquierda) y descifrado (derecha)	81
3.2.	Estructura del DEA . . . . .	84
3.3.	Descifrado e involución en el DEA, simplificado . . . . .	87
3.4.	Estructura de la función $F$ del DEA . . . . .	88
3.5.	Caja $E$ de expansión lineal de 32 a 48 bits . . . . .	88
3.6.	DEA reducido a dos vueltas . . . . .	94
3.7.	Cifrado múltiple . . . . .	100

3.8.	Ataque por encuentro a medio camino . . . . .	101
3.9.	TDEA . . . . .	103
3.10.	Esquema general del AES . . . . .	106
3.11.	Expansión de una clave AES de 128 bits . . . . .	111
3.12.	Expansión de una clave AES de 192 bits . . . . .	112
3.13.	Expansión de una clave AES de 256 bits . . . . .	112
4.1.	Cifrado y descifrado en modo ECB . . . . .	116
4.2.	Imagen tipo de mapa de bits (8 bits por píxel) . . . . .	117
4.3.	Cifrado y descifrado en modo CBC . . . . .	118
4.4.	Cifrado y descifrado en modo CFB . . . . .	120
4.5.	Cifrado y descifrado en modo OFB . . . . .	122
4.6.	Cifrado y descifrado en modo CTR . . . . .	124
4.7.	Modo de autenticación de mensaje CMAC . . . . .	126
4.8.	Diagrama de bloques de los modos de operación GCM y GMAC del AES . . . . .	127
4.9.	Cifrado y descifrado XTS-AES . . . . .	130
4.10.	Cifrado y descifrado XTS-AES, cuando el último bloque es incompleto . . . . .	130
5.1.	Ejemplo de generador seguro, combinando tres cifradores AES en modo contador . . . . .	158
8.1.	Curva elíptica $y^2 = x^3 - 12x + 4$ sobre $\mathbb{R}$ . . . . .	201
8.2.	Curva elíptica $y^2 = x^3 - 12x + 4$ sobre $\mathbb{F}_{23}$ . . . . .	202
8.3.	Suma de dos puntos distintos sobre $\mathbb{R}$ : $P + Q = R$ . . . . .	204
8.4.	Duplicación de un punto sobre $\mathbb{R}$ : $P + P = 2P = R$ . . . . .	205
8.5.	Suma de dos puntos distintos sobre $\mathbb{F}_{23}$ : $P + Q = R$ . . . . .	206
8.6.	Duplicación de un punto sobre $\mathbb{F}_{23}$ : $P + P = 2P = R$ . . . . .	207
8.7.	Esquema de cifrado ECIES . . . . .	214
8.8.	Esquema de descifrado ECIES . . . . .	215
8.9.	Curva hiperelíptica $y^2 = x^5 - 7x^3 + x^2 + 9x$ sobre $\mathbb{R}$ . . . . .	218
10.1.	Ejemplo de certificado X.509 . . . . .	251
10.2.	Espécimen del DNie . . . . .	253

---

10.3.	Anverso y reverso del DNIe . . . . .	254
10.4.	Tintas ópticamente variables . . . . .	254
10.5.	Imagen láser cambiante . . . . .	255
10.6.	Guilliches . . . . .	255
10.7.	Tintas visibles con luz ultravioleta o infrarroja . . . . .	256
10.8.	Fotografía . . . . .	256
10.9.	Solicitud de PIN . . . . .	258
10.10.	Actualización del PIN: conexión . . . . .	260
10.11.	Actualización del PIN: nuevo PIN . . . . .	261
10.12.	Puntos del permiso de conducir . . . . .	262
10.13.	Servicios de la Seguridad Social . . . . .	262
10.14.	Logotipo del pasaporte electrónico . . . . .	268
10.15.	Ejemplar de pasaporte electrónico . . . . .	269
10.16.	Imagen de don Quijote original y recuperada . . . . .	276
10.17.	Sombras de la imagen de don Quijote . . . . .	276
11.1.	Traza de potencia durante la ejecución del DEA . . . . .	286
11.2.	Traza de potencia durante la ejecución del RSA . . . . .	287