Indice generale

Nota dell'editore ..... **XIII**

Prefazione alla prima edizione ..... **XV**

Ringraziamenti per la prima edizione ..... **XVIII**

Prefazione alla nuova edizione ..... **XIX**

Ringraziamenti per la nuova edizione ..... **XXII**

Gli autori ..... **XXIII**

Parte I Introduzione

Capitolo 1 Il contesto della crittografia **3**

1.1 Il ruolo della crittografia 4
1.2 La proprietà dell'elemento più debole 5
1.3 Un ambiente ostile 6
1.4 Paranoia professionale 7
1.4.1 I vantaggi 8
1.4.2 Parlare degli attacchi 8
1.5 Il modello delle minacce 9
1.6 La crittografia non è la soluzione 11
1.7 La crittografia è molto difficile 11
1.8 La crittografia è la parte facile 12
1.9 Attacchi generici 12
1.10 La sicurezza e altri criteri di progettazione 13
1.10.1 Sicurezza e prestazioni 13
1.10.2 Sicurezza e funzionalità 15
1.10.3 Sicurezza e sistemi in evoluzione 15
1.11 Letture consigliate 16
1.12 Esercizi per la paranoia professionale 16
1.12.1 Esercizi su eventi dell'attualità 17
1.12.2 Esercizi sulle revisioni della sicurezza 17
1.13 Esercizi generali 18

Capitolo 2 Introduzione alla crittografia.....21
2.1 Cifratura 21
2.1.1 Il principio di Kerckhoff 22
2.2 Autenticazione 23
2.3 Cifratura a chiave pubblica 25
2.4 Firme digitali 26
2.5 Infrastruttura a chiave pubblica: PKI 27
2.6 Gli attacchi 28
2.6.1 Il modello con solo testo cifrato 28
2.6.2 Il modello con testo in chiaro noto 29
2.6.3 Il modello con testo in chiaro scelto 29
2.6.4 Il modello con testo cifrato scelto 30
2.6.5 L'obiettivo dell'attacco discriminante 30
2.6.6 Altri tipi di attacchi 31
2.7 Entriamo nei dettagli 31
2.7.1 Attacchi del compleanno 31
2.7.2 Attacchi meet-in-the-middle 32
2.8 Livelli di sicurezza 33
2.9 Prestazioni 34
2.10 Complessità 34
2.11 Esercizi 35

Parte II Sicurezza del messaggio.....37

Capitolo 3 Cifrari a blocchi 39
3.1 Che cos'è un cifrario a blocchi? 39
3.2 Tipi di attacchi 40
3.3 Il cifrario a blocchi ideale 41
3.4 Definizione di sicurezza dei cifrari a blocchi 42
3.4.1 Parità di una permutazione 44
3.5 Cifrari a blocchi reali 46
3.5.1 DES 46
3.5.2 AES 49
3.5.3 Serpent 51
3.5.4 Twofish 52
3.5.5 Altri finalisti per AES 53
3.5.6 Quale cifrario a blocchi scegliere? 53
3.5.7 Che lunghezza della chiave usare? 54
3.6 Esercizi 55

Capitolo 4 Le modalità dei cifrari a blocchi.....57
4.1 Riempimento 58
4.2 ECB 59
4.3 CBC 59
4.3.1 IV fisso 60
4.3.2 IV a contatore 60
4.3.3 IV casuale 60
4.3.4 IV generati da nonce 61
4.4 OFB 62
4.5 CTR 63
4.6 Cifratura e autenticazione insieme 64
4.7 Quale modalità utilizzare? 64

4.8 Fuga di informazioni ... 65
4.8.1 Probabilità di una collisione ... 66
4.8.2 Come gestire le fughe di informazioni ... 67
4.8.3 La matematica com'è trattata in questo libro ... 68
4.9 Esercizi ... 68

Capitolo 5 Le funzioni di hash ... 71
5.1 Sicurezza delle funzioni di hash ... 72
5.2 Funzioni di hash reali ... 74
5.2.1 Una funzione di hash semplice ma non sicura ... 74
5.2.2 MD5 ... 75
5.2.3 SHA-1 ... 75
5.2.4 SHA-224, SHA-256, SHA-384 e SHA-512 ... 76
5.3 Vulnerabilità delle funzioni di hash ... 77
5.3.1 Estensione della lunghezza ... 77
5.3.2 Collisione dei messaggi parziali ... 77
5.4 Rimediare ai punti deboli ... 78
5.4.1 Verso un rimedio a breve termine ... 78
5.4.2 Un rimedio a breve termine più efficiente ... 79
5.4.3 Un altro rimedio ... 80
5.5 Quale funzione di hash scegliere? ... 81
5.6 Esercizi ... 81

Capitolo 6 I codici di autenticazione dei messaggi ... 83
6.1 Azione di un MAC ... 83
6.2 Il MAC ideale e la sicurezza del MAC ... 84
6.3 CBC-MAC e CMAC ... 84
6.4 HMAC ... 87
6.5 GMAC ... 87
6.6 Quale MAC scegliere? ... 88
6.7 Utilizzo di un MAC ... 89
6.8 Esercizi ... 90

Capitolo 7 Il canale sicuro ... 93
7.1 Proprietà di un canale sicuro ... 93
7.1.1 I ruoli ... 93
7.1.2 La chiave ... 94
7.1.3 Sequenza o flusso ... 94
7.1.4 Proprietà di sicurezza ... 95
7.2 Ordine di autenticazione e cifratura ... 96
7.3 Progettazione di un canale sicuro: panoramica ... 98
7.3.1 Numerazione dei messaggi ... 98
7.3.2 Autenticazione ... 99
7.3.3 Cifratura ... 99
7.3.4 Formato del frame ... 100
7.4 Dettagli di progettazione ... 100
7.4.1 Inizializzazione ... 101
7.4.2 Invio di un messaggio ... 102
7.4.3 Ricezione di un messaggio ... 103
7.4.4 Ordinamento dei messaggi ... 104
7.5 Alternative ... 105
7.6 Esercizi ... 106

Capitolo 8 Aspetti relativi all'implementazione (I) 107
8.1 Creazione di programmi corretti 108
8.1.1 Le specifiche 109
8.1.2 Test e correzioni 110
8.1.3 Atteggiamento tollerante 110
8.1.4 Come procedere? 111
8.2 Creazione di software sicuro 111
8.3 Mantenere i segreti 112
8.3.1 Cancellazione dello stato 112
8.3.2 File di swapping 114
8.3.3 Memoria cache 115
8.3.4 Mantenimento dei dati in memoria 116
8.3.5 Accessi indesiderati 118
8.3.6 Integrità dei dati 119
8.3.7 Che cosa fare 119
8.4 Qualità del codice 120
8.4.1 Semplicità 120
8.4.2 Modularità 120
8.4.3 Asserzioni 121
8.4.4 Buffer overflow 122
8.4.5 I test 122
8.5 Attacchi a canale laterale 123
8.6 Conclusioni e altre letture 124
8.7 Esercizi 124

Parte III Negoziazione della chiave 125

Capitolo 9 Generazione di dati casuali 127
9.1 Casualità nei dati del mondo reale 128
9.1.1 Problemi nell'utilizzo di dati casuali reali 129
9.1.2 Dati pseudocasuali 129
9.1.3 Dati casuali reali e PRNG 130
9.2 Modelli di attacco per un PRNG 130
9.3 Fortuna 131
9.4 Il generatore 132
9.4.1 Inizializzazione 133
9.4.2 Nuovo seme 134
9.4.3 Generazione di blocchi 134
9.4.4 Generazione di dati casuali 135
9.4.5 Velocità del generatore 136
9.5 L'accumulatore 136
9.5.1 Sorgenti di entropia 136
9.5.2 Pool 137
9.5.3 Considerazioni sull'implementazione 139
9.5.4 Inizializzazione 141
9.5.5 Come ottenere dati casuali 141
9.5.6 Aggiunta di un evento 142
9.6 Gestione del file di seme 143
9.6.1 Scrittura di file di seme 144
9.6.2 Aggiornamento di file di seme 144
9.6.3 Quando leggere e scrivere sul file di seme 144

9.6.4 Backup e macchine virtuali ... 145
9.6.5 Atomicità degli aggiornamenti del file system ... 145
9.6.6 Il primo avvio ... 146
9.7 Scelta di elementi casuali ... 147
9.8 Esercizi ... 148

Capitolo 10 I numeri primi ... 149

10.1 Divisibilità e numeri primi ... 149
10.2 Generazione di numeri primi piccoli ... 151
10.3 Calcolo modulare con numeri primi ... 153
10.3.1 Addizione e sottrazione ... 154
10.3.2 Moltiplicazione ... 154
10.3.3 Gruppi e campi finiti ... 154
10.3.4 L'algoritmo per il massimo comun divisore ... 156
10.3.5 L'algoritmo di Euclide esteso ... 156
10.3.6 Calcolo modulo 2 ... 158
10.4 Numeri primi grandi ... 158
10.4.1 Test di primalità ... 160
10.4.2 Calcolo di potenze ... 163
10.5 Esercizi ... 164

Capitolo 11 Diffie-Hellman ... 165

11.1 I gruppi ... 166
11.2 Il protocollo DH originale ... 167
11.3 L'attacco man-in-the-middle ... 168
11.4 Trappole ... 169
11.5 Numeri primi sicuri ... 170
11.6 Utilizzo di un sottogruppo più piccolo ... 171
11.7 La dimensione di *p* ... 171
11.8 Regole pratiche ... 173
11.9 Che cosa può andare male? ... 174
11.10 Esercizi ... 176

Capitolo 12 RSA ... 177

12.1 Introduzione ... 177
12.2 Il teorema cinese del resto ... 178
12.2.1 La formula di Garner ... 178
12.2.2 Generalizzazioni ... 179
12.2.3 Impieghi ... 180
12.2.4 Conclusione ... 181
12.3 La moltiplicazione modulo *n* ... 181
12.4 Definizione di RSA ... 182
12.4.1 Firme digitali con RSA ... 182
12.4.2 Gli esponenti pubblici ... 182
12.4.3 La chiave privata ... 183
12.4.4 La dimensione di *n* ... 184
12.4.5 Generazione di chiavi RSA ... 185
12.5 I pericoli dell'utilizzo di RSA ... 186
12.6 Cifratura ... 187
12.7 Firme ... 190
12.8 Esercizi ... 192

Capitolo 13 Introduzione ai protocolli crittografici 193
13.1 I ruoli 193
13.2 La fiducia 194
13.2.1 Rischio 195
13.3 Gli incentivi 195
13.4 La fiducia nei protocolli crittografici 197
13.5 Messaggi e attività 198
13.5.1 Il livello di trasporto 198
13.5.2 Identità del protocollo e del messaggio 199
13.5.3 Codifica e analisi del messaggio 200
13.5.4 Stati di esecuzione del protocollo 200
13.5.5 Errori 201
13.5.6 Attacchi con replica e nuovi tentativi 202
13.6 Esercizi 204

Capitolo 14 Il protocollo di negoziazione della chiave 205
14.1 Lo scenario 205
14.2 Un primo tentativo 206
14.3 I protocolli sono eterni 207
14.4 Una convenzione di autenticazione 208
14.5 Un secondo tentativo 209
14.6 Un terzo tentativo 210
14.7 Il protocollo finale 211
14.8 Visioni diverse del protocollo 213
14.8.1 La visione di Alice 213
14.8.2 La visione di Bob 213
14.8.3 La visione dell'attaccante 214
14.8.4 Compromissione della chiave 215
14.9 Complessità computazionale del protocollo 215
14.9.1 Trucchi di ottimizzazione 216
14.10 Complessità del protocollo 217
14.11 Un avvertimento 218
14.12 Negoziazione della chiave a partire da una password 218
14.13 Esercizi 218

Capitolo 15 Aspetti relativi all'implementazione (II) 219
15.1 Calcoli aritmetici su interi grandi 219
15.1.1 Wooping 221
15.1.2 Verifica dei calcoli DH 223
15.1.3 Verifica della cifratura RSA 224
15.1.4 Verifica delle firme RSA 224
15.1.5 Conclusioni 224
15.2 Una moltiplicazione più rapida 224
15.3 Attacchi a canale laterale 225
15.3.1 Contromisure 226
15.4 I protocolli 227
15.4.1 Protocolli su un canale sicuro 228
15.4.2 Ricezione di un messaggio 228
15.4.3 Timeout 229
15.5 Esercizi 230

Parte IV Gestione delle chiavi 231

Capitolo 16 L'orologio 233

16.1 Impieghi di un orologio 233
16.1.1 Scadenza 233
16.1.2 Valore unico 234
16.1.3 Monotonicità 234
16.1.4 Transazioni in tempo reale 234
16.2 Utilizzo del chip RTC 235
16.3 Pericoli per la sicurezza 235
16.3.1 Portare indietro l'orologio 235
16.3.2 Fermare l'orologio 236
16.3.3 Portare avanti l'orologio 237
16.4 Creazione di un orologio affidabile 237
16.5 Il problema dello stato che non cambia 238
16.6 L'orario di riferimento 240
16.7 Conclusioni e consigli 240
16.8 Esercizi 241

Capitolo 17 Server di chiavi 243

17.1 Concetti di base 244
17.2 Kerberos 244
17.3 Soluzioni più semplici 245
17.3.1 Connessione sicura 245
17.3.2 Impostazione di una chiave 246
17.3.3 Rinnovo della chiave 246
17.3.4 Altre proprietà 246
17.4 Che cosa scegliere 247
17.5 Esercizi 247

Capitolo 18 Le PKI dei sogni 249

18.1 Breve panoramica sulle PKI 249
18.2 Esempi di PKI 250
18.2.1 La PKI universale 250
18.2.2 Accesso con VPN 250
18.2.3 Banca elettronica 250
18.2.4 Sensori di una raffineria 251
18.2.5 Circuiti di carte di credito 251
18.3 Altri elementi 251
18.3.1 Certificati multilivello 251
18.3.2 Scadenza 252
18.3.3 Autorità di registrazione separata 253
18.4 Riepilogo 254
18.5 Esercizi 254

Capitolo 19 Le PKI nella realtà 255

19.1 Nomi 255
19.2 Autorità 257
19.3 Fiducia 257
19.4 Autorizzazione indiretta 258
19.5 Autorizzazione diretta 259
19.6 Sistemi di credenziali 260

19.7 Il sogno rivisitato ... 261
19.8 La revoca ... 262
19.8.1 Elenco delle revoche ... 262
19.8.2 Scadenza rapida ... 263
19.8.3 Verifica di certificati online ... 263
19.8.4 Revoca obbligatoria ... 264
19.9 In conclusione, a che cosa serve una PKI? ... 264
19.10 Che cosa scegliere ... 266
19.11 Esercizi ... 266

Capitolo 20 Considerazioni pratiche sulle PKI ... 267
20.1 Il formato del certificato ... 267
20.1.1 Il linguaggio per i permessi ... 267
20.1.2 La chiave di root ... 268
20.2 La vita di una chiave ... 269
20.3 Perché le chiavi si usurano ... 270
20.4 Il cammino prosegue ... 271
20.5 Esercizi ... 271

Capitolo 21 Come conservare i segreti ... 273
21.1 Unità a disco ... 273
21.2 Memoria umana ... 274
21.2.1 Sale e allungamento ... 275
21.3 Supporti di archiviazione portatili ... 277
21.4 Dispositivi sicuri ... 278
21.5 Interfaccia utente sicura ... 279
21.6 Biometria ... 279
21.7 Sistemi SSO (Single Sign-On) ... 280
21.8 Rischio di perdita dei dati ... 281
21.9 Secret sharing ... 281
21.10 Cancellazione dei segreti ... 282
21.10.1 Carta ... 282
21.10.2 Supporti magnetici ... 283
21.10.3 Supporti a stato solido ... 284
21.11 Esercizi ... 284

Parte V Miscellanea ... 285

Capitolo 22 Standard e brevetti ... 287
22.1 Standard ... 287
22.1.1 Il processo di creazione degli standard ... 287
22.1.2 SSL ... 290
22.1.3 AES: standardizzazione attraverso la concorrenza ... 291
22.2 Brevetti ... 292

Capitolo 23 Rivolgersi agli esperti ... 293

Bibliografia ... 297

Indice analitico ... 305